## MATH 595: Quantum, Complexity, and Topology





Spring 2021 Eric Samperton University of Illinois

Meeting 1.1:			•
O. Welcome, logistics, 8	surveys		•
I. Course overview			•
I. What is a manifold?	>		•
II. Why are 3-dimensional	man: Folds special?		•
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		
Next time: Invariants	of manifolds, and	different	•
Next time: Invariants encoding:	of man: Folds, and s of 3-man: Fold	different S.	0 0 0 0
Next time: Invariants encoding:	of manifolds, and s of 3-manifold	different 5.	
Next time: Invariants encoding	of man: Folds, and s of 3-man: Fold	JiFferent 5.	
Next time: Invariants encoding:	of manifolds, and s of 3-manifold	Jifferent 5.	

I. Course overview
Goals:
- Understand the basics of quantum computing, computational Complexity,
and (geometric) topology (especially Knots and 3-manifolds).
- Build a precise picture of the role of topology in quantum computing,
especially as a source of quantum error correcting codes and potential
hardware applications via topological quantum computing.
- Develop analogies between reversible circuit models of
computation and topological invariants, especially those determined
by topological quantum Field theories (TQFTs).
- Review the state of the art in the complexity of various topological problems

Pra	ctically,	we wi	ll go ba	ackwards: top	ology First,	then CS,	then RC.	
	lecture	tor	Several	weeks, ac	eventually	we wil	1 frasition	
	Commun	9	zarnhg.					
· · · ·	· · · · · · ·	· · · ·	· · · · · · ·	· · · · · · · · ·	· · · · · · · · ·		· · · · · · · · ·	· · · · · · ·
	· · · · · · ·				· · · · · · · · · ·	· · · · · · ·		· · · · · · ·
· · · · ·	· · · · · · ·	· · · ·	· · · · · · ·	· · · · · · · · ·	· · · · · · · · · ·	· · · · · · ·	· · · · · · · · ·	· · · · · · ·
· · · · ·	· · · · · · ·	· · · ·	· · · · · · ·	· · · · · · · · · ·	· · · · · · · · · ·	· · · · · · ·	· · · · · · · · · ·	· · · · · · ·
	· · · · · ·			· · · · · · · · ·	· · · · · · · · ·	· · · · · · ·		
· · · ·	· · · · · · ·		· · · · · · ·	· · · · · · · · ·	· · · · · · · · ·		· · · · · · · · ·	· · · · · · ·
· · · · ·	· · · · · · ·	· · · ·	· · · · · · ·		· · · · · · · · · ·	· · · · · · ·	· · · · · · · · · ·	· · · · · · ·
				· · · · · · · · · ·	· · · · · · · · ·	· · · · · · ·	· · · · · · · · ·	

I. What is a manifold?
A topological space that has a reasonable, constant notion of
dimension, so every point has a neighborhood that looks like
a neighborhood of a point in IRM. More precisely:
Topological manifold of dimension in: Topological space Mn admits
an open cover { Ua} ac A together w/ coordinate charts, which
are homeomorphisms la: Ud > Va [ where Va is an open
set in IRM.
Typically also assume Mis Hausdorff and paracompact
Problem For computability: Honeo (IR") is gargantum.

Recall: the otlas of charts { Pa} determines a collection of trastion maps  $\Psi_{\alpha \rightarrow \beta} : \Psi_{\alpha} (U_{\alpha} \cap U_{\beta}) \rightarrow \Psi_{\beta} (U_{\alpha} \cap U_{\beta})$ "Better" manifolds are formed by requiring better conditions on all of the transition maps. Eig. the topol-gica manifold M is  $\psi_{\alpha} \rightarrow \beta$   $\psi_{\beta} \circ \psi_{\alpha}^{-1}(x)$ equipped w/ a smath structure it we pick an atlas of charts so that every transition map is 9 smooth function.  $(\mathcal{A}(\mathcal{V}_{\mathcal{A}} \cap \mathcal{V}_{\mathcal{P}}))$ 

Take-away: a topological manifold might have disterant
Smooth structures.
Even smooth manifolds are too complicated to teed to a
computer.
The "correct" type of manifold for inputting to computers is
piecewise linear. After massaging the tracition maps, we
Confeed flum to a computer.
But we can go fur ther! We can triagulate! Morrover, we get
special types of triagulations.

More precisely, every PL maitdo is PL homeomorphic to a	
Simplicial complex w/ condition that the link of every vert	EX
is q PL-sphere.	
A simplicial complex is a set of vertices together by	
a subset $C \subseteq P(V)$ that is downword closed.	· · · · · · ·
$\gamma = \xi = \xi = \xi = \xi$	
1 pre = { { a, b, c}, { { b, d} }	 
$C = \mathcal{P}(\{a_1, b_1, c, s\}) \cup \mathcal{P}(\{z, b_1, c, s\})$	· · · · · · ·
	· · · · · · ·
	· · · · · · · ·

Meeting 1.2	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	
L Triangulation	is of (compact,	PL) manifolds	· · · · · · · · · · · · · · · · · · ·
I. Basic ques	tions, and why	dimension 3 is	special
II. Time permitt	ting: other encoding	gs of Smanifolds,	Knots & links
Next time: ce	omplexity theory		

I. Triangulations
Recall our claim From last class: every (compact) PL
d-man; fold is PL-homeomorphic to a (tinite) d-dimensional Simplicial
Complex s.t. the link of every vertex is a PL d-1 sphere.
We will call such a simplicial complex a triangulation (of a
man: Fold)
Link of vertex v is the union of all simplices
T such that I and V share a simplex, but I
and v are disjoint. $ink(v) = $
$\sim$

PL Homeomorphism
A homeomorphism F: M -> N is a PL homeomorphism, it
in all coordinate charts (of the PL structures of M and N),
F is a PL homeo b/w open subsets of Rh.
Two triangulations are combinatorially equivalent it they
have isomorphic refinements.
Let Ti be a triangulation of Min i=lid. The e-g.
Then M, and My are PL (-Fi-1) (-Fi-1)
homeomorphic it and only it
To and The are combinatorially
equivalet.

Example	Every 2	-regular gr	aph is	a triange	lation	of a	(possil	y)	
disconnec	ted) +	mas: Fold.							
			2 4 100	copies	F St	· · · · · ·	· · · · · ·		
									• • •
· · · · · · · ·		· · · · · · · · · · · · · · · · · · ·	· · · · · · ·	· · · · · · ·		· · · · · ·	· · · · · ·		
Example	Every	2-dim si	mplicial	complex	where	each	edge		
is Cont	aired in	exactly	L triano	les is	a tric	ngulatio		9	
is cont	ained in	exactly ?	L triano	yles is man: Fold"	9 tric	ngulatio		9 	· · ·
is cont Svrface	ai-ed in (Surface)	exactly à	L triano lensioma) u	yles is man: Fold"	a tric ).	ngv/atio	े गै	7	
is cont Svrface	ai-ed in ("surface"	exactly dim	L triano .ens:ong) u	yles is mon:told"	9 1000).	ngv/afio		9	
is cont Svrface	ai-ed in (Surface)	exactly ; = "2 - dim	L triano lens:ong) u	yles is man: Fold"	9 1000).	zgv/atio		9	
is cont Svrface	ai-ed in ("surface"	exactly : = "2 - dim	L triano	yles is man: Fold"	9 (ric ).	~gv/afi*		<b>7</b>	
is cont Svrface	ai-ed in ("surface")	exactly ?	L triano	yles is mon:Fold"	9 (ric	~gv/~fi*		<b>7</b>	
is cont Svrface	ai-ed in ("surface")	exactly ?	L triano	yles is man: Fold"	9 tric	∼g ∪ / ۹ f i •		7	



Warning A simplicial complex may be homeomorphic (but yot PL homeomorphic) to a man: Fold, even if the complex is not what we're calling a triangulation.						
Double	<u>suspens</u> his the	sion theorem	omology a	is 504 5 52	d-man: Fold then the	
double	susper	sion ot	M <sub>1</sub> S	$\mathcal{A}\mathcal{M}_{1}$ i	s a topo bi	gical
9+7	sphre.	· · · · · · · · · ·	· · · · · · · · · · ·			
	· · · · · · · ·		· · · · · · · · · · ·			

ManiFolds with boundary In defin of manifold, just replace Rd with Rd-1 x [0, 20). <u>Example</u> P P --triangulation of torus u/ one boundary component For friangulations of manifolds w/ boundary, the links of boundary points should be d-1 distrs.

Standing implicit assumptions					
Abuse of	notation "man fold"	will offen mean	friangulation of 9		
(closed, ca	ompact, orientable)	man: Fold.			
But some	times not.	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		
If unclear,	please ask!	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		
· · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		
· · · · · · · · · · · ·					
· · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		
· · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·			

II. Basic questions, and my d=3 is the best (to me)
If we want to use triangulations of manifolds as input to
computer programs designed to calculate properties of manifolds,
at the very least, we would like to recognize when a
simplicial complex is a valid friagulation.
How would we do thus?
Work recursively and "down" From d all the way to O.
Pick a vertex V and calculate link (J).
Then determine it link (US is a (d-1)-dimensional friangulation,
IF not, stop. IF yes, then decide if link(u) is a d-1
sphere. If yes, more to next vertex. Repeato

The curse of a	uncomputability 6M	en a d-manitold, ic i	t a d-sphere?
λ.	d-sphere recognition	(d +1) - dimon sion a) I ciangulation recognition	d-martild house 0.
	easy easy easy	E 939 E 73-1	e asy easy Rasy *
3 4	NP n co NPt No IDEAS	algorithmically possible Fort not ensy	Algorithmic, but Complexity unknown
	NOT POJSIBLE ?? -		
(*): First dec (t): will c	ide if 2-manitold; the discuss noxt week	r compute Hx Usi	ng SNF on d, cellier boundary anop.

Other nice things about 3-manifolds Moise's Theorem In dimension 3  $\nabla T = P = D$ TOP = PL = DIFF.Poincaré conjecture true  $\vec{s}$  T = P = D $4 \vec{s}$   $T \neq P = D$ IF M is has homotopy groups of S<sup>3</sup>, then M=S<sup>3</sup>. 51 ZTFPCD Exotic sphones. Ocometrization V

Meeting 2.1: Other 3-manifold encodings I. Heegnard splittings and diagrams
II. Knots and links: stick presentations and diagrams III. Bridge position, braid growns, and trace closures
Skipping For now: surgery presentations of 3-manifolds Next time: structure of 3-manifolds
Announcements: - office half hour on Wednesdays, 3:30-4:00. w/ option to go extra half hour
- Class will end today at 3pm.

I. Heegaard splittings and diagrams A handle body of genus q is a 3-manifold homeomorphic to a regular neighborhood of a wedge of g circles in IR3. () BE(P) (E Small enargh) pEWrdge Let M be a (closed, or:etable) 3-anonit-10. A Heegaard surface (or Heegaard splittung) is an embedded contract ( r ... some genes of such that cutting M along S' Cesults in two handlebodies. "(it Malang S' means "M-N(S).")

Lemma Every (closed, orientable) 3-momitold has a Heegaard surface. More precisely, if T is a triangulation of a 3-monthly with t fetrahedra, then Y has Hecgoard surface of genus = # 71 - # Max Tree (7-1). y = one skeleton Remark: the gove will typically be way tagger than necessary. We define genus (M3) to be the minimum genus of all Hergarand splittings of M. gerus (M3) is an invariant.

Proof by picture S= JN(T'). We need let For Heegoard Surface, to check that each piece of Y-S is a hadebody of genus #7'= #Max Tree (7) We can contract any maximal free in Ho to get 9 homeounglic marifold. By Construction the 3-manded is a wedge of # 41 - # Max Tre (71) many circles.  $H = N(\gamma')$ 

Note that HI= Y- Ho has boundary S. To see that it is a 3-manifold hamous expluse to q regular ubbid of a graph, look at dual one skeleton

Ve wat to recover a 3-monitold from a sortace (which will be the Heegaard splitting) + Finite amount of extra data Defin Call q collection of curves c1, C21 -- , Cy on a genus q surface S a complete disk system (F: i) Ci's pair vise disjourd ii)  $\int - (\frac{1}{2}) c_i$  is connected. There Let S be a gewis g surface with a complete disk system (1,--r cg. Then, up to have our phicum re) S, there is a unique hardlebody H with 214 = S such this each ci bounds an embedded dist.

Skitch of proof SX[-1,0] Similarly over here glue: D<sup>2</sup>x[-1,1] So D<sup>2</sup>x {0} is idet! Fied w/c,  $ON(c_i)$  $D = \bigcup_{x \in -1, +1}^{3}$ 

· ·				ĥ	ور	ر ۲	•	•		$\mathcal{S}$	, 1 1	ر					(	ĺ		)	•		د ا د	· · ·		7	· · ·	Ċ	)	· ·	5		re	ŗŗĕ	2,-	• •	· · ·	•	•	• •	· ·	•	· · ·	•	•
• •			) ¢	)	•	+	, <b>,</b>	•	6	5 ( ) (	ie.	ţ.c	у Т	- - - - -	י י י	•	β				ן בר ו	°√ √	' ¦∽	g	•	•	دے م	<u>لم</u>	p	r JI	, . , .	¥	4	י ר ר	•			0 0	e A	; <b>U</b>			· ·	•	•
• •		0'	r V	•	Ľ	ie	'nγ	•	· ·	f	<b>-</b>	•	g		e C	•	• •	9	•	•		ζ,		L	י רי ר	[ <sup>1</sup>   	· ·	•	$\frac{1}{2}$	b b		•	D	) (	י גר ו		S.	<b>^</b>	۱ ۱	)	).	•	<b>7</b>	•	•
•	•	•	•	•	•	•	•	•	· ·	•	•	•	•	•	•	•	· ·		•	•	•	•	•	· ·	•	•	• •	•	•	•		•	• •	•	•	• •		•	•	• •	· ·	•		) }	•
••••	0	•		0			0	0	• •	0	0	0	0	•	•	0			•	•	•	0	•	•••	0	•	•••	0	•	•	•	•	•••	•	0	• •	 	0	•	• •	• •	•	• •	•	•
• •	0	•		0	•	•	0	•	• •	•	0	0	0	•	•	0			•	•	•	0	•	0 0 0 0 0 0	0	•	• •	0 0 0	•	0		0	• •	•	0	• •	0 0 0 0	0	0	• •	• •	•	• •		•
• •	•	•	•	•	•	•	•	•	· ·	•	•	•	•	•	•	•	· ·		•	•	•	•	•	• •	•	•	· ·	•	•	•		•	• •	•	•	• •	· ·	•	•	• •	· ·	•	· ·	•	•
• •	•	•	•	0	•	•	•	•	· ·	•	0	0	•	•	•	•			•	•	•	•	•	• •	•	•	· ·	•	•	•		0	• •	•	•	• •	· ·	•	•	• •	· ·	•	· ·	•	•
• •	0	•	•	•	•	•	•	•	••••	•	•	•	•	•	•	•			•	•	•	•	•	••••	•	•	• •	•	•	•	•	•	••••	•	•	• •		•	•	• •	• •	•	• •	•	•

Corollary Every closed oristable 3-manitold can be presided as a Heegerard diagram, which consists of a surface S of some genus 9, together u/ two complete disk system on S In fact, S can be tringulated, and each curve in the disk systems is a normal curve.

Example(			· · · · ·			· · · ·	· · ·	· ·
	<u> </u>	  	· · · · ·	· · · ·		· · · ·	· · ·	· ·
k	>	· · · · ·	· · · · ·			· · · ·	· · ·	• •
		· · · · ·	· · · · ·	· · · ·		· · · ·	· · ·	• •
		· · · · ·	· · · · ·	· · · ·		· · · ·	· · ·	• •
	C		· · · · ·			· · · ·		
	$\mathcal{I}$	· · · · ·	· · · · ·		· · ·	· · · ·	· · ·	
	· · · · · · · · ·	 	· · · · ·			· · · ·	· · ·	· ·
	 					• • •		

	Meeting 2.2: More on 3-manifold encodings I. Normal curves and Heegaard diagrams II. Knots and links: stick presentations and diagrams																																										
· · · · · · · · · · · · · · · · · · ·	N J	e 7	d E	ر ۲	~ <i>E</i>	ek P	< •	۱. ۲	(	50 br	lv an	۰ ۲ ۲		د ب ا	)   	ſ		-1 -1 	5 5 5	90 79	ار م لامہ	) 	26		ч ч	, t	) )	_ fl	5+1 -ei	;}.	ure Co	, • • • •		3	- 	<i>ب</i>	Ge '	fo		シ	)	•	•
		• •	•										•							•										•							•						
																						• •								•										• •			
		• •		• •				• •				•	•	• •		•	•					• •						• •				•		•					•	• •			
							•																													•				• •			
				• •										• •								• •						• •															
				• •										• •								• •						• •					•	•			•	•	•	• •			
				• •			•	• •			•		•	• •		•	•					• •						• •	•		• •	•							•	• •			
-			-																					-											-								

I. Normal curves and theegood diagrams Last time: Corollary Every closed orsutable 3-manitold can be presented as a Heegenerd diagram, which consists of a surface S of some genus 9, together u/ two complete disk systems on S In fact, S can be triagulated, and each curve in the disk systems (ay be made a normal curve.

More examples: SXS  $= S^2 \times S' # S^2 \times S'$ lgreen curve bounds disk on both sides Corrigonds to a 2-sphere embedded in M

Connect sums of manifolds: Let M, N be two orientable 3-folds (connected). Pick MEM, NEN. Let  $M' = M - \overline{R_{\varepsilon}(m)}, N' = N - \overline{R_{\varepsilon}(n)}$ M'and N' cade his a new S2 bandary comparet. B/c ormadely, we can identify two copies of S2 in 9 M (M) (M) Unique way

Let M#N lae  $M' \sqcup N'$ JM' - JN' Conversely: a 3-manifold L is a connect sun precisely when there exists an embedded d-sphere S<sup>2</sup>CL s.t. neither component at L-S2 is a 3-ball.

More examples: every monitold with a genus one splitting is called a lens space: L(3,2)- ( a build L(m, m) for any min. 5 00 - Classified up to homeomorphicm Non-homeomorphic les spaces can be homotopy equivalent.

Let's compute something.  $\left( A \right) = L(3,2)$ =  $A UB A nB = S' YS', A = B = S' + B^2$ Mayor - Viotoris sequence  $H_1(A \cdot B) \rightarrow H_1(A) \oplus H_1(B) \rightarrow H_1(L) \rightarrow 0$  $\mathbb{Z} \otimes \mathbb{Z} \xrightarrow{(3)} \mathbb{Z} \oplus \mathbb{Z} \longrightarrow \mathbb{Z}/3$ <-> @<b>
Normal Curves Let Y be a triangulated surface. A curve & is normal (wit Y) if every segment in J-T' has its endpoints on distinct edges of 71, and Ruling out curves 6000' that backtrack

Normal curves Up to isotopy in T-T, a normal curve is detormined by a vector of edge intersection courts: Vy: Edges (T) -> Z20  $V_{\chi}(E) = \# \gamma n E$ Consider 

Normal curves The set of (isotopy classes rel To of) normal curves is a polyhedral cone in 2 Edges. Claim: a vector v & Dedges determines a normal curve it and only it, for each triangle TET, the there corresponding entries of V satisfy tringle equalities" ei ez 355 1 7 C

	<u>e</u> e	+: N K B	<u>n «</u> ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	j S J	<u> </u>	<u>)</u> .	<u>)</u> - p	را را	N /e= :			e S	。 よ、 こ、	۲ (۲	f-1 k		~ 79 (e	n <i>qi</i> 94 5 4	ai o P	F0 70	1 1 1	lic	e g s a	رم ر م	c nu a	, o , o +	) ( <b>1</b>	کے م	íq	g' C	- 91   0	 SV	( ( e	* * * * * * * * * * *			· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		
Next week: 1. Complexity theory (not structure of 3-montoloc) 2. Example problems for 3-manitolds and their complexities.																																								
		• •		•							•		•		• •											•	• •				• •						• •	 	•	
		• •		•				•	• •						• •				•	•	•				•		• •				• •				•	•	• •			•
									• •											•														•				 	•	
	•	• •							• •				•		• •												• •			•							• •	 		
	•	• •		•			•		• •	•				•	• •	•				•			•			•	• •		•	•						•	• •			
									• •												•								•		• •						• •			
																																					. ,	 		
		• •							• •				•		• •												• •									•	• •			

Warning	
Triangulation >> Heegaard diagram easy, but	· · · · · · · · · · · · ·
Converse is usually expensive.	· · · · · · · · · · · · · ·
Problem: a normal curve vator V G Z Zo	· · · · · · · · · · · · · ·
can encode a curve that is exponentially long	· · · · · · · · · · · · ·
in the size of V.	· · · · · · · · · · · ·
Take-awayi Hoeysand	
diagram is	· · · · · · · · · · · · · ·
"highly compressed	· · · · · · · · · · · · ·
AAV	· · · · · · · · · · · · · ·

De ciding hompomorphism From Heegaard diagrams <u>Reidemeister - Singer</u> Two Heeggand diagrams represent homeour orphic manifolds if and obility if they can be identified by a sequence of elementary operations. I. Isotopy ). Handle slide 

3. Stabilization destatilize

II. Knots and links: stick presentations and diagrams A knot is a continuos injection (eurbedding)  $K: S' \rightarrow \mathbb{R}^3$  (or  $S^3$ ). Often, contlate a Knot K with its image. When are two knots equivalent? One wrong answer: isotopy. Recall, two maps KIL: SI > R's are isotopic if there is a continual Function H: S'x EOI) -> IR > Such that H/SIX { 03 = K and H/S'X { 13 = L,

and H(-,t) for any fixed t is an embedding. Why is thic wrong? Can use 14 to shrint the interesting, Isotopins can unite Knots trivial! Dat

One correct definition = quibient isotopy	· ·	· · ·	• •
Kand Lare quitient isotopic if there exists	• •	· · ·	• •
$H: \mathbb{R}^3 \times [O_1 \mathbb{R}] \longrightarrow \mathbb{R}^3$	· ·	· · ·	• •
such that	• •	· · ·	• •
i) H (-it) is a homeomorphism of R3	· ·	· · ·	• •
$ii \int H(-,0) = 10_{R3}$	• •	· · ·	• •
$iii) H(K(x), I) = [(x) Foc all x \in S]$	· ·	· · ·	· ·
	· ·	· · ·	• •
· · · · · · · · · · · · · · · · · · ·	• •	· · ·	• •
· · · · · · · · · · · · · · · · · · ·	· ·	· · ·	· ·

Another correct detriction: Homeomorphism! Say Kad Love homeomorphic et there exists  $L: \mathbb{R}^3 \xrightarrow{\simeq} \mathbb{R}^3$ such that h(K(x)) = L(x)) for all  $x \in S'$ . Two definitions ALMOST identical: every orientation precerving homeo of  $M^{2}$  (or  $S^{3}$ ) is isotopic to the identity. (left-handed US (ight-handed tretails) Ex: Gus Co

<u>Me</u>	<u>eti</u>	ng J	3.	<u> </u> ,	)  	1. (	· · ·	•		•		•	· ·	· · ·	1	L	• •		•	· · ·		· · ·	•	· · ·	•	· · ·	•	•	· ·	•	•	· ·		· ·	•
Т.	r. I	ne (2 ) ) ) (i)	s Ige	~°	) )o	(i~1) s:7(	15	•	57	(C - 91	r J	f	9(	5 <i>e</i> 9V	ار کو کو	91	ເຈັ 1	an	ð	- -	- -	0 7 P			م م د د	)re	٤	•	•	•	•	· ·	•	· · ·	•
· · ·	• •	· · ·	• •		• •	•	• •	•	• •	•	• •		• •		• •		• •		•	• •	•	• •	•	• •	•	• •	0	•		•	0	• •	•	• •	•
· · ·	• •	· · ·	• •		• •		• •	•	• •	•	• •	•	• •	•	• •	•	• •		•	• •	•	• •	•	• •	•	· ·	•	•		•	•	• •	•	••••	•
· · · ·	• •	· · · ·	• •		• •	•	· ·	•	· ·	•	· ·	•	· ·	•	• •	•	• •		•	• •	•	· ·	•	· ·	•	· ·	•	•	• •	•	•	• •	•	· ·	•
· · ·	· ·	· · · ·	• •		· ·	•	· ·	•	· ·	•	· ·	•	· ·	•	• •	•	· ·		•	· ·	•	· ·	•	· ·	•	· ·	•	•	•	•	•	· ·	•	· ·	•
· · · ·	· ·	· · · ·			· ·	•	· ·	•	· ·	•	· ·	•	· ·	•	· ·	•	• •		•	· ·	•	· ·	•	· ·	•	· ·	•	•	•	•	•	· ·	•	· ·	•
· · ·	· ·	· · · ·	• •	1 0 1 0	· ·	•	· ·	•	· ·	•	· ·	•	· ·	•	• •	•	• •		•	• •	•	· ·	•	· ·	•	· ·	•	•	•	•	•	· ·	•	· ·	•
							• •	•	• •	•	• •	•	• •	•		•			•		•	• •	•		•	• •	•				•	• •	•		•

Recall, a knot is a cts embedding. K: SI->S <sup>3</sup> A knot is the if it comes from costricting a embedding N(K): SIXD> > S <sup>3</sup> Via N(K)   SIX{0}. "Tome" = "Has a tubular meighborhood" A knot that is not town is called wild. Any knot K that Extends across a distrinic an unknot. That is if there exists a cubedding T: D <sup>2</sup> = S <sup>3</sup> such that T   D <sup>2</sup> = T   S' = K.	I. Knots and links: stick presentations and diagrams
K: S'→S <sup>3</sup> A knot is there if it comes from restricting a embedding N(K): S'×D→→S <sup>3</sup> Via N(K) S'×{0}. "Tome" = "Hos a tubular neighbor hood" A knot that is not town is called wild. Any knot K that "extends across a distrinic is an unknot. That is if there exists a cubedding T: D→→S <sup>3</sup> such that T D→ = T S' = K.	Recall, a knit is a cts embedding
A knot is time if it comes from restricting a embedding N(K): SIXD> => S3 Via N(K)   SIX{0}. "Tame" = "Has a tubular meighborhood" A knot that is not town is called wild. Any knot K that "extends across a distriction on another. That is if there exists a embedding T: D= => S3 such that T   D= = T   S' = K.	$K: S' \rightarrow S^3$
$N(K): SIXD^{2} \rightarrow S^{3}$ Via $N(K)   S^{1} \times \{0\}.$ "Tome" = "Has a tubular neighborhood" A knot that is not four is called wild. Any knot K that Extends across a distrinis an unknot. That is if there exists an curbedding $T: D^{2} \rightarrow S^{3}$ such that $T   dD^{2} = T   S^{1} = K$ .	A knot is trane if it comes from cestricting a embedding
Via $N(k)   S' \times \{0\}$ . "Tame" = "Has a tubular neighborhood" A knot that is not town is called wild. Any knot K that Extends across a Jisti" is an unknot. That is if there exists a curbedding $T: D^2 \rightarrow S^3$ such that $T   D^2 = T   S' = K$ .	$N(\mathbf{k}): S^{1} \times \mathbb{D}^{2} \rightarrow S^{2}$
"Tame" = "Has a tubular neighborhood" A knot that is not four is called wild. Any knot K that "Extends across a disti" is an unknot. That is if there exists a curbedding T: Da => S3 such that TIADa = TIS' = K.	$Vig N(k)   S' \times \{o\}.$
A knot that is not tome is called wild. Any knot K that Extends across a district of an unknot. That is if there exists an embedding $T: D^2 \rightarrow S^3$ such that $T[D^2 = T[S] = K$ .	"Tame" = "Has a tubular meighborhood"
Any knot K that Extends across a districit an unknot. That is if there exists an embedding T: Da => S3 such that T[]Da = T[s' = K.	A knot that is not form is called wild.
That is if there exists a cubedding $T: D^2 \rightarrow S^3$ such that $T[dD^2 = T[S] = K$ .	Any knot K that Extends across a district an unknot.
$f_{Lat} = T  _{\partial D^{a}} = T  _{S'} = K.$	That is if three exists an embedding T: Da > S3 such
	$I_{1} + T_{1} = T_{1} = K$



Tome knots are always isolopic to PL knots JESO: YPES!  $[K(p), K(p+E)] \subseteq Image(N)$ 

Stick presentations and triagle moves A stick presentation of a kat is a sequence of points PoiPiin, PL=Po E Z<sup>3</sup> CR<sup>3</sup> CS<sup>3</sup> so that For all 1, j = 0, ..., L-1, the line segments PiPiti and PiPiti have disjont interiors and P; = P;

A tringle two stick	move is an presentations:	elemetar.	isotopy	between
·       ·	Piti	Qí	· · · · · · · · · · · · · · · · · · ·	Qita Pity
		$\longrightarrow$		
		·       ·		
P <sub>1</sub>			Č.	$b_{i} = A_{i}$

IF Q is any post in 23 such that the trivole Pi QPiti is disjont From all at the other sticks, then two stick presentations related by a triangle move represent intopic knots Theor Two stick presentations represent equivalent knots (ambient isotopic) it and only it they are celated by a sequence at tringle moves.

Diagrams and Reidemeinter moves A diagram of a knot is an enbedded planar graph with extra information at vertices to encode crossing information. This planar graph shald came tran a regular projection of a knot K in R3 oute a plane. - Require preimage of every point to have at most 2 pauls / - Wo're force of -Also don't allow crossing singularities to tonsverse (

Diagrams and Reidemeinter moves The Two knot diagrams represent equivalent knots iff they are related a sequence of Reidenneistin movers: Type I THE SAN MAN  $\mathcal{D}$ 

Type I	$\sum_{n} \left( \sqrt{n} \right) \left( \sqrt{n} \right)$
Type II (brogp celetion)	

I. Bridge position, braid groups, and trace closures														
A Frot diagr	A knot diagram is in <u>bridge position</u> it, when													
Considered as	s q subjet	of xy-plane,	all of the											
fraxime OCC	cur qt same	height, and	all of the											
migim g		· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·											

Proposition Given any knot diagram, we can ensily Find a equivalent diagram in bridge position. Proof:

Artis braid group (s) By is the brand group on a strands, which is presented vig 6; 5; = 5; 5; iF [i-j]>  $B_{n} = \{ \sigma_{1}, \sigma_{2}, \dots, \sigma_{n-1} \} = \sigma_{j} \sigma_{j+1} \sigma_{j} = \sigma_{j+1} \sigma_{j} \sigma_{j+1} \forall i \}$ We can interpret a string of only as a picture of a braid; the celefions ever that isotopic broads are considered equal elements of the group.

Ex Consider 0,02020201 in By Convention: "Right to left" = "Bottom to top" 03 Or 52 02 1 Z Of ا م (iteral equality in group corresponds to kotopy of braid diagons

Given my word in the generators of By
We can draw a braid dragram.
Furthermore, if n=21% is over, the following three
pieces of data give us a diagram of a knot in
Lridge position:
1. (ups (a place matching of the dir strands)
J. Caps (J; Ho)
3. A word in generators of Bax.

Warning: Previous Cecipic might yield 9 link Liggram instead of a Knot diagram. Alternative construction : Trace closure. Given braid word w C Bur do His? 

Tue trace obsures of braids represent equivalent links when they are related by a sequence of two types of moves  $\left| \begin{array}{c} (\sigma_{j} u g^{\alpha_{j}} c_{j} \\ \ddots \\ \end{array} \right|^{2} \chi_{w} \chi^{-1} \left( \begin{array}{c} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \right) \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \begin{array}{c} \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \\ \cdots \\ \end{array} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \end{array} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \end{array} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \end{array} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j}} c_{j} \right)^{2} \left( \left( \sigma_{j} u g^{\alpha_{j$ 2. Stalization: 

, like Reidemeister 2. Stalization:

•	Meeting 3.2: A smattering of complexity																																									
•	I. Decision problems, counting problems, and computability																																									
	Л	-	Ĩ	- L	e	, U	ŝU	9		•گ	ν̈́ς	• <b>•</b> ••	e	- 1:	5:	• •	P.	-	F	> 	N	P	, P	۹2	A	c E	Ξ,	E	X	P	#		1	Ē	R	, 1	٩,	R	E		• •	
•	U		Ŕ	Ze	du	ردآ	t: e	54	S	•	ه	2	•	h.	9 / I	) n	یک ا	\$	•	• •	• •	•	•	•	• •			• •	•	• •		• •	•	0	• •		•	• •	•		• •	0
•	• •					0		• •				• •			•				0			0								• •		• •			• •				•			
					• •			• •				• •									• •						•	• •		• •					• •			• •			• •	
	• •				• •			• •				• •				• •				•	• •				• •		•			• •		• •			• •			• •			• •	•
•								• •				• •				• •					• •				• •							• •						• •			• •	
	• •							• •				• •								•	• •																				• •	
				•	• •			• •				• •				• •				•	• •				• •		•			• •					• •			• •			• •	
•	• •			•	• •			• •			•	• •				• •				•	• •				• •		•	• •		• •		• •			• •			• •			• •	
	• •							• •				•				• •				•	• •				• •					• •		• •			•			• •			• •	
	• •							• •				• •				• •														• •								• •		•		
								• •				• •													• •																	
	• •						•	• •				• •				• •									• •										• •			• •				

I. Decision problems, counting problems, and computability A decision problem is a function les L: {0,13\*= () {0,13\*-> {0,13} k21 · · · · · Ala A counting problem is a turction F: {0,13\* ~> {0,1}\*= N, in binory Remark: the domain of a problem, nonely {0113, is typically an encoding of some interesting combinationialized mithematical object.

Typical we don't care too much about details of
how to encode a "combinatorialized unthematical object" into
a bit string, so long as
1. The encoding is "efficient
2. Deciding if a but string represents a valid object is
$e_{\gamma}$
Example: ve con creade simplicial complexes in bit
Stribus in such a manar
Non-example: We can not encode triangulations of 6-dimensional
PL monitolde in such a Fashier.
· · · · · · · · · · · · · · · · · · ·
Stribus in such a manner <u>Non-example</u> : We can not encode triangulations of 6 dimensional PL manitolds in such a tashion.

Before daing complex: Computatility.	+- <i>γ</i> , ι	re n	eer to	undesta	
Turing Machines	are	Ore	way to	make	
algorithms precise	• • • • •	· · · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · · · ·
	· · · · ·				
	· · · ·	· · · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · · · ·
	· · · · ·				
	· · · · ·	· · · · · · ·	· · · · · · · ·	· · · · · · · · · ·	
		· · · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · · · ·

Turing Machines defin From Arora + Barak's Computitional Complexity **Formal definition.** Formally, a TM M is described by a tuple  $(\Gamma, Q, \delta)$  containing: A finite set  $\Gamma$  of the symbols that M's tapes can contain. We assume that  $\Gamma$  contains a

• A finite set  $\Gamma$  of the symbols that M's tapes can contain. We assume that  $\Gamma$  contains a designated "blank" symbol, denoted  $\Box$ ; a designated "start" symbol, denoted  $\triangleright$ ; and the numbers 0 and 1. We call  $\Gamma$  the *alphabet* of M.

• A finite set Q of possible states M's register can be in. We assume that Q contains a designated start state, denoted  $q_{start}$ , and a designated halting state, denoted  $q_{halt}$ .

A function  $\delta: Q \times \Gamma^k \to Q \times \Gamma^{k-1} \times \{L, S, R\}^k$ , where  $k \ge 2$ , describing the rules M use in performing each step. This function is called the *transition function* of M (see Figure 1.2.)

																- A charge	IF	
																	Input	W
																	symbol	ou
																1. Aller	Tead	syi
																to the law of the		rea
							•									1 Barris		
•																	: Alterna	
																0435 Jac 1.	and a state	3.0
																	a	22
		•							•	•	•	•	•	•	•	anonno	an north	12.2
																	1	-
							•											
							•									m bailing	C. Houles	1
																and Friday and		-

			THEN									
Input symbol read	Work/ output tape symbol read	Current state	Move input head	New work/ output tape symbol	Move work/ output tape	New state						
1	: 	A The	in i page	a spool	:	1						
а	Ъ	q	Right →	b'	Left	q'						
i	:	in Baffacea	(chena)	101-102 	in a set of							

"Read-Write"

head fint moves Left + Righ

Figure 1.2. The transition function of a two-tape TM (i.e., a TM with one input tape and one work/output tape)

Input topp **1** 0 **1 -**0 Work lope output (eg) -wr . . . . fet+Woret right

This is an important model, with some artigrary
Cho:ces.
(hurdh - Turing Thesis: Computable dors not depend
on model of computations
Extended Church - Turing Thesis: "Eff: cully computable"
does not depend on the model of computation,
as long as its <i>reollstic</i> .
Problen: Quatur computers.
I. Usual suspects
---
A complexity class is any cet of (decision or counting)
problems. Typically interested in complexity classes
defined by restraining the resources used by a
Turing marchane (space, time, etc)
Will start at the Top."
RE: recusively enumerable decision problems.
LERE if there exists a Turing madule sit.
For all $X \in \{0, 1\}^{4}$ , if $L(X) = Yes, then$
the Turing anachine returns Yes when input x
and every the "HALT" state.

Example: Halting Problem.
Given a Turing machine T, detirance it
Thalts when input an empty string.
In RE because we can tuild a Turing machine
that curs other Furing mading inside of it
(Universal Turne unduke)
Example (Homomophism problem for PL-manitolds)
L: {0,13 * x {0,13 * -> { Yes, No}
L(X,y) = S Yos IF x and y reprocent transventions of PL
No otherwise. maissides that are PL-haream-phic
· · · · · · · · · · · · · · · · · · ·

c.RE	: Some as	REbut	surap colro	F YES and No.
R:	Cecursive	for computa	ble) Fundiors,	Joned 67
· · · · · · · · · ·	R=	- REnc	ORE	· · · · · · · · · · · · · · · · · · ·
Intuteu:	a problem	is in R	IF there is a	way to soke
. 1	1 I.			
;+	algor: thm: (	cally but wy	1 No bounds o	m (esources
;+ (eq	algor: thm: ( Uired,	call-11 but w	1 uso bounds o	M (esources
;t (eg	algor: thm: ( Uired,	call-11 60+ ~1	1 No bounds o	M (esources
;+ Ceg	algor: thm: ( Uired,	call-11 60+ ~1	1 Wo bounds o	M (esources
;+ Ceg	algor: thm: ( Uired,	call-11 60t vy	1 wso bounds o	M (esources
;+ (eg	algor: thm: ( Uired,	call-11 60t vy	1 No bounds o	M (esources
;+ Ceg	algor: thin: ( Uired,	call-11 60t vy	1 wso bounds o	M (esources
;+ Ceg	algor: Hum: ( Uired,	call-11 60t vy	1 No bonds o	M (esources
;+ Ceg	algor: Hum: ( Uired:	call-11 60t ~1	1 NSO Gourds 0	M (esources

Non-examples	Noith	Halt-s Problems	nor Home O.
Problem for	PL-marit	folds is in R.	
Example. 3-	- MariFold	Homeomorphism	Pro blen
L: {0,13 *	× {0,1}*	~ { Yes, No }	
	0		
= (×, y) =	{ Yes	17 Xiy repres	I handonorphic 3 maitolds
L (×, y) =	{ Yes No	otherwise	I handonopluc 3 maitolds

Meet	ing	4.1	A su	ngttering	f co	mplex: +1	1 continued	· · · · · · · · · · · · · · · · · · ·
Į.T	he	USUA	Suspe	ets: P	, <mark>FP</mark> , N	P, PSPACE	E, EXP, #P,	ER, R, RE
<u>Ш</u> . R	Led	rctions	5 ~ 2	hardnes	 S		· · · · · · · · · · ·	
	• •							
	• •							
· · · · · ·	• •		· · · · ·	· · · · · · ·	· · · · · ·	· · · · · · · ·		
· · · · · ·	• •	· · · ·	· · · · ·	· · · · · · ·	· · · · · ·	· · · · · · · ·	· · · · · · · · · ·	
· · · · · ·		· · · ·	· · · · · ·	· · · · · · ·	· · · · · ·	· · · · · · · ·	· · · · · · · · · ·	
	• •					· · · · · · · ·		
	• •	· · · ·		· · · · · · ·	· · · · · ·	· · · · · · · ·	· · · · · · · · · · ·	
	• •							· · · · · · · · · · · · · · ·

Note PENPEPSPACEEEXPEERERE
Except Here
FR: elementary recursive Functions To unnach, lette
have TIME (F(h)) be g/1 decision problems that Can be called an Turine machine that was in time
O(F(n)), where h is the size (i.e. lensth) of input.
$\mathcal{L}(\mathcal{H}(\mathcal{U}, \mathcal{H}))$ can be define $\mathcal{L}(\mathcal{L}(\mathcal{H}))$ .

Then  $ER = \bigcup TIME \left( \int_{k=1}^{k=1} d^{k-1} \right)$ Nice exercise:  $ER = U SPACE ( j^{2})$  $\left( \text{SPACE}(n) \subseteq \text{TIME}(\lambda^{n}) \right)$ 

Ex 3-Monifold Homeomorphism (There of G. L: {0,13* x{0,13* -> } yes, No }
L(XIY) = { les 1F x ad y encode haveo. Imavitolog No otherwise
Why? Geometrization: every 3-manitold can be cut up into pieces in a canonical way so each piece can be
endoured with one of 8 Thurston geometries (IE3, S3, H3,)
Iden et algorithmi geometrize X and y in parsillel, then Compare their geometric pieces.

$E \times P = \bigcup TIME (2^{k}) = 2^{O(poly(m))}$ $kz_{1}$
$PSPACE = () SPACE(u^{k})$ $k \ge 1$
PSPACE SEXP (Note: if we need print space For an algorithm, the Turing machine running the algorithm can be in at most O(I <sup>print</sup> ) possible configurations.)
P= () TIME (nk). If a problem is in Pr we k=1 consider it efficiently solvable.

NP: non deterministic polynomial time.
We say LENP if thre exists TM M and two
polynomials p(1), 7(1) such that for all input x
to Lot length n=
1. IF L(x) = Yes, then exists y E E0,13 such that
$\mathcal{M}(x_{1}y) = Yes.$
2. IF L(x)=No, M(x,y)=No tor all yE {0,139(m)
3. M(xiy) (uns in time p(h) for all ye { 0/1} 7(h).
For such of Turing another we can call the
YEZOIIZZIN "proofs" or "intresses" or "centicates."
(They are not trustworthy, and M tests their credibility.)

Example SAT ("Booleon Sertistiability")
hstances of SAT are Boolen tormulas, e.g.
$(\times \vee_{\gamma} \vee_{z}) \wedge (\langle s \vee_{\gamma} \vee_{z} \rangle)$
Preliemi given a Boolean tormula $f(x_1, x_2,, x_n)$ , decide 17 there is a input such that $F$ evaluates to ( (or "True") or that input.
Why is SAT in NP? Take the different possible input to Fas the certificates.
(F SAT (F): Yes, then of carse some input to F evaluates to True. And of cause if SAT (F): No, no input will fool the procedure.

Ex Graph 3-colorability
Instance: Graph F, e.g. as adjacency matrix
Problem: Decide if I has a valid vertex 3-coloring.
Witness: $p: V(\Gamma) \rightarrow \{R, G, B\}$
Oiven a vitness, we can quickly verity whether or not
it yields valid graph coloring.
Given a vitness, we can quickly verity whether or not it yields valid graph coloring.
it yields valid graph coloring.
Viven a vitness, we can quickly verity whether or not it yields valid graph coloring.

Ex Knot 3-coloral:1:ty
Instance. Knot diagram.
Problem: Decide it we can color connected arcs of diagram
with 3-colors so at each crossing, either 3 colors
are seen, or just 1. Also require that we use all
3 colors.
Oray! Okay! [270]

Vitnesses: p: {arrs} ~ {R,G,B}	7 Ca	chock i	
.       .	7.t	3-color cble	• • • • • • • • • • • • •

II. Reductions and hardness Given two problems Loud K, 9 Korp (eduction r is polynomial time computeble Function such that For all XE { O(1} we have L(x) = K(r(x)). {0,1}\* -> { Yes, No} r 1 { 0,13 \* K Such an r is a reduction From L to K. We interpret K as being at least as hard as L.

Another type of reduction:
polynomial-time Turing reductions (alka "Code reductions")
Given a problem K, an oracle Turing machine For K
is a usual Turing machine, together up a black box
that solves instances of K in one time step.
pK = all problems solvable in poly from on a Turing
machine w/ oracle for K.
We say L is Cook reducible to K IF LEPK.
$\left( \begin{array}{c} c \end{array} \right) = \left( \begin{array}{c} c \end{array} \right) \left($

A problem K is NP-hard iF for all LENP, there exis	f1
- Karp reduction From L to K. IF, moreover, KE.	VP,
We say K is NP-complete.	· · · · ·
	· · · · ·
101-complete in NP + NP-hard"	· · · · ·
NP-had is trasitive under Korp reduction.	· · · · ·
Theorem (Cook - Levin)	· · · ·
SAT is NP-complete.	· · · · ·
So is 3-SAT	· · · · ·
· · · · · · · · · · · · · · · · · · ·	· · · ·

Ex (de Mesuray, Rieck, Sea	Swick, Tomerr)
Trivial Sublink problem is	NP-complete.
Instance: a link diagram L	and natural number in
Problem: decide if L has an	n-component Unlink that
is a trivial lak.	
· · · · · · · · · · · · · · · · · · ·	
$\mathcal{E}$	



Meeting 4.2: The complexity of unknot recognition I. In NP via normal surface theory (Hass-Lagariss-Pippenger, after Haka) I. In NP Via Reideneister moves (Lackenby) II. In CONP, Modulo GRH (Kuperberg) IV. In CONA (Lockenby) Next week: granting mechanics and grantum computing

Problem: Unknot Recognition Instance: Knot diagram K Question: Is K the Unknot?	· · · ·
K is an unknot if: 1. it's equivalent under a sequence of Reidemeister mares	•
to a diagram Nat crossings 2. if K bounds an embedded dist	•
3. $\pi_1(S^3-K) \cong \mathbb{Z}_r$ :-finite cyclic group	•
	•

I. In NP via norma	I surface theory (Hass-Lagariss-Pippenger)
The Computational Complexity of K	not and Link
Problems	Journal of the ACM, Vol. 46, No. 2, March 1999, pp. 185–211.
JOEL HASS	
University of California Davis Davis California	
. University of California, Davis, Davis, California	
JEFFREY C. LAGARIAS	
AT&T Laboratories, Florham Park, New Jersey	In this paper, we consider knots and links as represented by link diagrams and
AND	computational problem of recognizing unknotted polygons as follows:
NICHOLAS PIPPENGER	computational problem of recognizing unknotted polygons as follows.
University of British Columbia, Vancouver, BC, Canada	Problem: UNKNOTTING PROBLEM
	Instance: A link diagram D
	Question: Is $\mathfrak{D}$ a knot diagram that represents the trivial knot?
	See Welch [1002a, 1002a] for more information on this problem. The main
	see weish [1995a-1995c] for more mornation on this problem. The main
	result of this paper is the following.
	THEOREM 1.1 The UNKNOTTING PROBLEM is in NP.
	The UNKNOTTING PROBLEM was shown to be decidable by Haken [1961]; the
	result was announced in 1954, and the proof published in 1961. From then until
	now, we know of no strengthening of Haken's decision procedure to give an
	explicit complexity bound. We present such a bound in Theorem 8.1
	enpiere comprenie, council ne present such a councilin metrem on

Given V, triagulated 3-manifold, u	re Can	desc	r.be	· · ·	
"normal surfaces" using certain vector	s 27	も /	whre	· · ·	
t is # tetra hedrog in Y.					
Inside each tetrahedron True have 7	+ types	A	element		
dichs=			· · · · · · ·		
3'	· · · · · · · ·		· · · · · · ·	· · ·	• • •
	$\mathbf{O} = \mathbf{O} + $	• • •	· · · · · · ·	· · ·	
		· · ·	· · · · · · ·	· · ·	
	gunds	• • •	· · · · · · ·	· · ·	
· · · · · · · · · · · · · · · · · · ·		· · ·	· · · · · · ·	· · ·	· · ·

A vector ve 2<sup>3t</sup> determins a normal surface if •  $V_i \ge 0$  for each  $i = 1, \dots, 7t$ · "mostching condition" for each pair of taxes that are glued together of the form  $V_{i_1} + v_{i_2} = V_{\ell_1} + V_{\ell_2}$ · "quid condition": For each tetrahedron, see at most one grad type



Basic iden: effectivizing Haken's normal Surface theory
1. Given K, a Knot diagram with h crossings, Can
build triangulation of MK = S3-N(K) in time O(n log n)
with t= O(n) tetrahedra, in standard way.
Certificate: A vector VEZ7t ad a list of Zt-1
linear constracts, with Vi E 27t-1
]. Test that v encodes a normal surface by verify.
it satisfies:
it satisties: "matching equations" Detine Hatron's normal Detine Hatron's normal Detine Hatron's normal
it satisfies: • matching equations" • positivity: Vi 20 Vi=1,, 7t Detre Haten's normal (one CM in R7t
it satisfies: • "matching equations" • positivity: vi 20 Vi=1,, 7t Detine Chain R7t • "guad Conditions" Nothear, but easy to chart

3. Verify the 7t-1 linear constraints are independent, V satisfies them, and gcd (VI, -1, Vyt) = [. This shows V is a Vertex minimal integer point in CM. 4. Vertex minimality ensures V represents a connected Mormal sur Face. Now check v represents a disk (compute X) and has correct boundary on  $\partial M_{k} = S' \times S'$  (theck  $(\partial v) = (0,1) \in H_{1}(S' \times S')$ ). Procedure works by theorem of Jaco - Tolletson Saying if K is Unknot, it has a vertex minimal disk. HLP showed there  $e_{x:st}$  one  $\sqrt{v_i} \leq \frac{1}{2}$ .

· · · · **.** . . . . . . . . . . . . . . .

```
. . . . . . .
```

I. In NP via Reideneister moves (Lackenby

Annals of Mathematics **182** (2015), 491–564 http://dx.doi.org/10.4007/annals.2015.182.2.3

## A polynomial upper bound on Reidemeister moves

## By MARC LACKENBY

THEOREM 1.1. Let D be a diagram of the unknot with c crossings. Then there is a sequence of at most  $(236 c)^{11}$  Reidemeister moves that transforms D into the trivial diagram. Moreover, every diagram in this sequence has at most  $(7 c)^2$  crossings.

Subtle	Warning:	·       ·
<b>Theorem</b> using at r	<b>1.</b> Given an unknot diagram $D$ and an integer $k$ , deciding nost $k$ Reidemeister moves is <b>NP</b> -complete.	$ng \ if \ D \ can \ be \ untangled$
	Advances in Mathematics 381 (2021) 107648	Moral
	Contents lists available at ScienceDirect Advances in Mathematics	Optimal unknoting
	ELSEVIER www.elsevier.com/locate/aim	Via Reideneight
	The unbearable hardness of unknotting ☆ Arnaud de Mesmay <sup>a,*</sup> , Yo'av Rieck <sup>b,*</sup> , Eric Sedgwick <sup>c,*</sup> , Martin Tancer <sup>d,*</sup>	Morves is N/A-1
	<sup>a</sup> Université Paris-Est, LIGM, CNRS, ENPC, ESIEE Paris, UPEM, Marne-la-Vallée, France <sup>b</sup> Department of Mathematical Sciences, University of Arkansas, Fayetteville, AR 72701, USA <sup>c</sup> School of Computing, DePaul University, 243 S. Wabash Ave, Chicago, IL 60604, USA	() - ha-d
	<sup>~</sup> Department of Applied Mathematics, Charles University, Malostranské nám. 25, 118 00 Praha 1, Czech Republic 	· · · · · · · · · · · · · · · · · · ·

II. In CONP, Modulo GRH (A	uperberg)
Opposite question (Knotledness detection) Instaxe: Knot diagram K	Advances in Mathematics 256 (2014) 493–506 Contents lists available at ScienceDirect Advances in Mathematics ELSEVIER www.elsevier.com/locate/aire
Question: Is K Not the chknot?	Knottedness is in NP, modulo GRH Greg Kuperberg <sup>1</sup> Department of Mathematics, University of California, Davis, CA 95616, United States

**Theorem 1.1.** Let  $K \subset S^3$  be a knot described by a knot diagram, a generalized triangulation, or an incomplete Heegaard diagram. Then the assertion that K is knotted is in NP, assuming the generalized Riemann hypothesis (GRH).

Together with Hass–Lagarias–Pippenger, we can restate the result as

											J	Jn	kr	10	tte	ed	ne	$\mathbf{SS}$	$\in$	N	P	$\cap c$	NP,	
•	•	•	•	•	•	•	•	• •		•		•	•	•	•	•	•			•	•		Problems in here a	re
	•			•	•			· ·	•	•		•			•								believed not to be	NP-hard.

Our proof of Theorem 1.1 quickly follows from major results of others. Kronheimer and Mrowka [20] showed that if K is a non-trivial knot, then there is a non-commutative representation of i.e. image et Pr is non aber

 $\rho_{\mathbb{C}}: \pi_1(S^3 \setminus K) \to \mathrm{SU}(2) \subset \mathrm{SL}(2, \mathbb{C}).$ 

Then, simply because the equations for the representation are algebraic, the complex numbers can be replaced by a finite field  $\mathbb{Z}/p$ . Koiran [19] showed that if a polynomiallength set of algebraic equations has a complex solution, and if GRH is true, then there is a suitable prime p with only polynomially many digits. Thus, the certificate is a prime p and a 2  $\times$  2 matrix over  $\mathbb{Z}/p$  for each generator of the knot group. The verifier must check that the generator matrices satisfy the relations of the knot group; and that they do not all commute, or in the Wirtinger presentation, that they are not all equal. This confirms that K cannot be the unknot.

																					Contents lists available at ScienceDirect		
																					Advances in Mathematics	Manazourics	
																				ELSEVIER	www.elsevier.com/locate/aim		
	•			•	• •	• •			• •			• •				•	• •			Knottedness is	in NP, modulo GRH		
									•			• •			•		• •			Greg Kuperberg <sup>1</sup>	m m , mouno crur		
	•								• •											Department of Mathema	tics, University of California, Davis, CA 95616, United States		

	\ \			 		 
(V. In CONA () me Ken	·~ )			 		 
THE EFFICIENT CERTIFIC	ATION (	$\mathbf{F}$		 		 
KNOTTEDNESS AND THUR	TON NC	)PM		 		 
			• • • •	 • • •	• • • •	 
MARC LACKENBY	1020	00000	t	 • • •	• • • •	 
		T. L.	×	 • • •		 
		• • • •		 • • •	• • • •	 
				 • • •		 
				 • • •		 
		• • • •	• • • •	 • • •	• • • •	 
				 • • •		 
				 0 0 0		 

<u>Meeting 5.1</u> : I. The postule	Quantum Me	chanics	·         ·	·         ·	·       ·	
Section 2.2 c	of Nielsen -r	Chuang	·         ·	· · · · · · · · ·	·       ·	
Quantu Computat	m tion	.       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .         .       <	.       .       .       .       .       .         .       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .	· · · · · · · · · · · · · · · · · · ·		
MICHAEL A. NIE and ISAAC L. CH	ion USEN UANG	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · ·	.       .	
		· · · · · · · · · · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · ·	·       ·	
CAMBRIDGE		· · · · · · · ·	· · · · · · · ·	· · · · · · · ·	· · · · · · · · · · · · · ·	

I. Postulates of quantum mechanics
1. What we quantum states?
In How can quantum states evolve over theme?
3. How do we measure quatur states and how are
quatum states affected by measurement?
4. What do composite systems look like?
The axions specify the mothematica) Frame work for assuring
these questions. The work of a physicist is to understand,
tor a specific system, what the spectric mathematica) objects are.
We will take a practical mathematical approach to the axions,
and ignare (at least for now) their physical just Frontion (e.g. Bell inequilities
Dirac bra-ket ystation

Con Use that F notation F and the m

Notation	Description
	Complex conjugate of the complex number $z$ .
	$(1+i)^* = 1-i$
$ \psi angle$	Vector. Also known as a ket.
$\langle \psi  $	Vector dual to $ \psi\rangle$ . Also known as a <i>bra</i> .
$\langle \varphi   \psi  angle$	Inner product between the vectors $ \varphi\rangle$ and $ \psi\rangle$ .
$ arphi angle\otimes \psi angle$	Tensor product of $ \varphi\rangle$ and $ \psi\rangle$ .
$ arphi angle \psi angle$	Abbreviated notation for tensor product of $ \varphi\rangle$ and $ \psi\rangle$ .
$A^*$	Complex conjugate of the A matrix.
$A^T$	Transpose of the A matrix.
$A^{\dagger}$	Hermitian conjugate or adjoint of the A matrix, $A^{\dagger} = (A^T)^*$ .
ps	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{\dagger} = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}.$
$\langle \varphi   A   \psi \rangle$	Inner product between $ \varphi\rangle$ and $A \psi\rangle$ .
	Equivalently, inner product between $A^{\dagger} \varphi\rangle$ and $ \psi\rangle$ .

1. States are vectors in a Hilbert space complete
<b>Postulate 1</b> : Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the <i>state space</i> of the system. The system is completely described by its <i>state vector</i> , which is a unit vector in the system's state space.
Often, but not always, a state space also has a preferred basis
("computation) 6asis")
Waraha : Dalike in classical computing
a chile is the list of a Stringtal The
$q \leq  q  e \qquad (\leq y_0, q) \qquad   s  \qquad 0  (oe)  (de)  (de) $
Coefficients can be computed, but we will get to ethat
· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·

Examples: quaite, quiters, quaits, quaits	· · · · · · · ·
A qubit is any quartum system and a dimensional	state
space, typically with a preferred basis	· · · · · · · ·
In other words, [2 = span [ { 107, 11} ; a	qubit.
o-thomormal basis	· · · · · · · ·
(10) = (10) =	· · · · · · · ·
C P = C	· · · · · · · ·
Qupit: (1 - Spon 2 107,, [p-17], p prime	
Qudit: Cd= spon { [0],, [d-17], m-1 d.	

Amplitudes IF 107,, 12-17 is an ONB and
14)= Sailis is any nonzero vector, we
call the ai's (Unnormalized) quantum amplitudes.
Normalizing and projectivizing
If 147 is not unit length but is at least nonzero,
then 14) is a state.
Well see shorthy, that scalar moltiples can't be distinguished,
Mixed states so we could define state space as projective space.
These are classical mixtures of quantum states

2. Time evolution is a Uniter frastarmation

**Postulate 2**: The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state  $|\psi\rangle$  of the system at time  $t_1$  is related to the state  $|\psi'\rangle$  of the system at time  $t_2$  by a unitary operator U which depends only on the times  $t_1$  and  $t_2$ ,

$$|\psi'\rangle = U|\psi\rangle \,.$$

"Infinitasimal Version">

(2.84)

(2.86)

Constant in

Global Version

Postulate 2': The time evolution of the state of a closed quantum system is described by the *Schrödinger equation*,

 $i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle.$ 

In this equation,  $\hbar$  is a physical constant known as *Planck's constant* whose value must be experimentally determined. The exact value is not important to us. In practice, it is common to absorb the factor  $\hbar$  into H, effectively setting  $\hbar = 1$ . H is a fixed Hermitian operator known as the *Hamiltonian* of the closed system.

Examples of Unitary time evolution For 9 gubit  $\begin{array}{c} T = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ Pouli operators  $\frac{|I|}{5} = \frac{1}{\sqrt{2}} \begin{pmatrix} |I| \\ |-I| \end{pmatrix} X also called "bit Flip"$ H tor "Hadonmard," Not Hand Horian! 2 called "(relative) phase Flip" (no classical anlog)  $\frac{1}{2} | 0 \rangle = | 0 \rangle_1 \frac{1}{2} | 1 \rangle = -11 \rangle_1 \frac{1}{2} \left( \frac{10 + 11 \gamma}{\sqrt{2}} \right) = \frac{10 \gamma - 11 \gamma}{\sqrt{2}}$ 

Han: Itonians and energy eigenstates (iver eigenvectors of Harmitian operators)
A Homiltonian is simply a self-adjoint operator H.
(H <sup>t</sup> = H), intended to encode the energies of
States
E:genectors are called energy eigenstates.
Recall: H is diagonalizable with real spectrum.
The eigenvalues of H are the "energy puels" of
the system.
· · · · · · · · · · · · · · · · · · ·

Different: ote Global (nfinitesime) Version Integrate/Solve Schrödinger equition  $i = \frac{d | \Psi(t) \rangle}{dt} = \frac{H}{4}$ Unitory!  $\frac{d \left| \psi(t) \right\rangle}{dt} \approx -\frac{iH}{t_1} \left| \psi(t) \right\rangle$  $|\gamma(t)\rangle = \int_{0}^{t} -\frac{iH}{t} |\gamma(\tilde{t})\rangle d\tilde{t} = \left[e^{-\frac{itH}{t}}\right] |\gamma(0)\rangle$ 

3. Measurements are certain collections of linear operators (XXX)

**Postulate 3**: Quantum measurements are described by a collection  $\{M_m\}$  of *measurement operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is  $|\psi\rangle$  immediately before the measurement then the probability that result m occurs is

given by

$$p(m) = \langle \psi | M_m^{\dagger} M_m | \psi \rangle , \qquad (2.92)$$

(2.93)

(2.94)

and the state of the system after the measurement is

$$rac{M_m |\psi
angle}{\sqrt{\langle \psi | M_m^\dagger M_m |\psi
angle}} \ .$$

The measurement operators satisfy the completeness equation,

$$\sum M_m^{\dagger} M_m = I \,.$$

Example: Measuring a qubit in computational basis
$\mathcal{M}_{0} =  0\rangle\langle 0  = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},  \mathcal{M}_{1} =  1\rangle\langle 1  = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$
$N_{o} = M_{o}^{t} = M_{o}^{t} = M_{o}^{t} = M_{o}^{t} = M_{o}^{t} = M_{o}^{t}$
but this need not be the case for general measurements.
Completeness equation follows immediately
$E_{.g.}$ $ 4\rangle = \frac{1}{\sqrt{5}} (2 0\rangle - 3 1\rangle)$
Prob 147 wints up in state 1: { IF 147 does vind up in state 1, then its state is
$\langle \Psi   M_0^{t} M_0   \Psi \rangle = \langle \Psi   M_0   \Psi \rangle$ =

Mensurements can not detect global phose Mus measured on 147 US. e<sup>i0</sup>147:  $(e^{i\theta}(\psi))^{t} = \langle \psi | e^{-i\theta}$  so {24/e-i0 Mt Musei0/27 = {24/Mus Mus 127) <u>Take-away</u>: Since measurements carlt distinguish scalar multiples of a state, we should consider them physically indistinguishable.

Measurements can relicity distinguish orthogonal vectors
Given orthogonal normal states 124,7 and 14,2,
cre can prepare measurements
$M_{1} =  \gamma_{1}\rangle\langle\gamma_{1} , \qquad M_{2} =  \gamma_{2}\rangle\langle\gamma_{1} $
and $M_0 = I - M_1 - M_2$ .
You can check that the probability distributions
are: with the second se
are: $w_1 = w_1 =$

Box 2.3: Proof that non-orthogonal states can't be reliably distinguished

Measurements can probabilistically distinguish independent vectors

A proof by contradiction shows that no measurement distinguishing the nonorthogonal states  $|\psi_1\rangle$  and  $|\psi_2\rangle$  is possible. Suppose such a measurement is possible. If the state  $|\psi_1\rangle$  ( $|\psi_2\rangle$ ) is prepared then the probability of measuring j such that f(j) = 1 (f(j) = 2) must be 1. Defining  $E_i \equiv \sum_{j:f(j)=i} M_j^{\dagger} M_j$ , these observations may be written as:

 $\langle \psi_1 | E_1 | \psi_1 \rangle = 1; \quad \langle \psi_2 | E_2 | \psi_2 \rangle = 1.$  (2.99)

Since  $\sum_i E_i = I$  it follows that  $\sum_i \langle \psi_1 | E_i | \psi_1 \rangle = 1$ , and since  $\langle \psi_1 | E_1 | \psi_1 \rangle = 1$ we must have  $\langle \psi_1 | E_2 | \psi_1 \rangle = 0$ , and thus  $\sqrt{E_2} | \psi_1 \rangle = 0$ . Suppose we decompose  $|\psi_2 \rangle = \alpha |\psi_1 \rangle + \beta |\varphi\rangle$ , where  $|\varphi\rangle$  is orthonormal to  $|\psi_1 \rangle$ ,  $|\alpha|^2 + |\beta|^2 = 1$ , and  $|\beta| < 1$  since  $|\psi_1 \rangle$  and  $|\psi_2 \rangle$  are not orthogonal. Then  $\sqrt{E_2} |\psi_2 \rangle = \beta \sqrt{E_2} |\varphi\rangle$ , which implies a contradiction with (2.99), as

$$\langle \psi_2 | E_2 | \psi_2 \rangle = |\beta|^2 \langle \varphi | E_2 | \varphi \rangle \le |\beta|^2 < 1, \tag{2.100}$$

where the second last inequality follows from the observation that

 $\langle \varphi | E_2 | \varphi \rangle \le \sum_i \langle \varphi | E_i | \varphi \rangle = \langle \varphi | \varphi \rangle = 1.$  (2.101)

**Projective measurements**: A projective measurement is described by an *observable*, M, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition,

3. Measurements can be understood from "projective menuruts" (\*\*\*)

$$M = \sum_{m} m P_m \,, \tag{2.102}$$

where  $P_m$  is the projector onto the eigenspace of M with eigenvalue m. The possible outcomes of the measurement correspond to the eigenvalues, m, of the observable. Upon measuring the state  $|\psi\rangle$ , the probability of getting result m is

given by

$$p(m) = \langle \psi | P_m | \psi \rangle . \tag{2.103}$$

(2.104)

Given that outcome m occurred, the state of the quantum system immediately after the measurement is

 $P_m |\psi\rangle$ 

p(m)

Statistics are easy to extract from projective measurements Expectation value of M in state 147:  $\mathbb{E}(\mathcal{M}) = \sum_{m} m p^{(m)} = \sum_{m} \sqrt{24} P_m \sqrt{24}$  $=\langle \mathcal{Y}|\Sigma_{m}P_{m}|\mathcal{Y}\rangle$ Standard deviation: = (7/117).  $\Delta(m)$  $= \mathbb{E}(M)^{2} - \mathbb{E}(M^{2}) = ((M^{1}M^{1}M^{2}))^{2} - (2M^{2}M^{2})^{2}$ Heisenberg uncertainty:  $\Delta(c)\Delta(D) \ge \frac{[\langle 4|[c_iD]]4\rangle]}{2}$ Proof: Use Cauchy - Schurge 2 ...-

Examples Pauli operators! Every Herenitan operator on C <sup>2</sup> is a IR-linear contination of Pauli operators. or I+6X+cY+dZ	
Hamiltonians are energy obsorvables (that's My they control dynamics Allow us to answer questions like: "Given state 147, that is the probability it has a certain energy?"	<b>)</b>

tensor Aroducts g/e T. Lomposite tems

**Postulate 4**: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state  $|\psi_i\rangle$ , then the joint state of the total system is  $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ .

IF system A described by Hilbert space	? Å,	4 1 1 1 1	· ·	• •	· •
$\mathcal{B}$	HB	,	· · ·	· · ·	· · ·
then the composite system AB is	  	· · · ·	· · ·	• •	· ·
AB:=HA & HB.	  	· · · ·	· · ·	· · ·	· ·

Curse of dimensionality (blessing?) State space of n quaits is  $( \begin{array}{c} & & \\ &$ n times JN d'imension

mixed states and Difference b/w entended states. Not I the Form IF INDE HA WH B 1247 014B7, We say 147 is entryled. A mixed state in H is gime by dereity opporator  $\mathcal{A} \otimes \mathcal{B}$ B(H) = mixed states Malgebra of openaters

Meeting 5.2: Digging into quantum states
I. "Completely understanding" of guantum state
I. No closing
II. Distinguishing states, Cedux
IV. Some good news: the Deutsch - Jozsa algor: Hum.
· · · · · · · · · · · · · · · · · · ·
Next time: Quantum circuits as model of quantum computers, and BQP.
Next time: Quantum circuits as model of quantum computers, and BQP. Note: live given up telling myself I'm going to Tex separate notes.

Summary of axions of quantum mechanics: 1. States are nonzero (unit) vectors in a Hilbert space. 2. Physica) tractormations of closed systems are unitary. 3. A quatum state 147 nd measurement & Moj..., MK3 determine a probability distribution on 20,..., k}. 4. Composite sustems are tensor products.

I. "Completely understanding" a quantum starte
In classical computer with an n-bit memory register it is easy to read off
information that completely determines the register's state: just read each
each bit one after the other.
This is NDT true of quantum systems.
Suppose we have an n qubit system (thought of as a quantum
memory) which is in a state $  \gamma \rangle E(\mathbb{C}^{2})^{\otimes n}$ .
How can we convince ourselves we completely understand 197?
It depends on 1977 and what we mean by "Completely understand."

One iden: determine all of the coefficients of 14)
in a preferred basis.
OF course, MY can be made part of some basis,
but our "preferred basis" shouldn't depend on 127).
For a gubsts, we use the tubor product basis as
our computational basis.
$ O\rangle = (000) =  0\rangle \otimes  0\rangle \otimes \otimes  0\rangle E([0)) \otimes u$
> = (00 ··· 1> = (0) 02 107 00 ··· 00 11> / 000 quanter terois
12) = 10 10) = 10> @ @ 11) @ 10> (~h if the )
States, an tell
$ N-1\rangle = (1 -1) = (1) \otimes (1) \otimes - \otimes (17) \text{ where } N = 2^{n}$ .) is which one.

In principle, we know there exist an N-1 E I such fligt
$ \Psi\rangle = \sum_{i=1}^{n} a_i  i\rangle_i \sum_{i=1}^{n}  a_i ^2 = 1.$
tou do me determine the a;?
Well, there are exponentially many! So let's try For go only
We need to Find some measurement or observable that
will help us determine 90.
OF course,
a = <0/4>, so we could fry
$M_0 =  07\langle 0 , M_1 = I -  07\langle 0 .$
$ = \left[ $

With this measurement, probability of getting outcome O on 1247 is
$p(0) = \langle \Psi   M_0   \Psi \rangle$ (note $M_0 = projector$ )
= <4 10> <0 12>
$= \gamma_0^* \gamma_0$
$= \left  \alpha_0 \right ^{\lambda}$
So, with this choice of measurement, the best we can
do is see 1901 as a probability of a certain at come.
It Turns out, with a little bit more cleverness, we cand determine the late bit has a context of
just to know the probability. How can we really do that?

Well, if we make the above measurement, either
we get autcome O with probability proj = /00/2, or
we get outcome I with probability
p(1) = (4/M, 14) = (4/(I-10)(0)) 4)
$= \langle 4   I   4 \rangle - \langle 4   0 \times 0   4 \rangle$
$=  \gamma  ^{2} -  \gamma_{0} ^{2}$
$=  - q_0 d$
Performing this measurement only once, we can't expect
to determine anything beyond whether it seems, probabilistically
that 190/2712 or 190/2 = 1/2.
It we want to do better, we have to do another measurement!

But the First measurement spoiled 147 [F we got out come O, then 147 has be ingote into 0). IF we got outcome I, then 147 is now in state  $\frac{M_{1}147}{\sqrt{p(1)^{2}}} = \frac{1}{\sqrt{1-\ln^{2}}} \left( 147 - \alpha_{0} | 07 \right) = | 1 \right)$ In the First Case, if we perform the measurement again on the new state, we of course just get back 10>. Likewise, in the second case,  $M_{o}\left(\frac{M_{1}|W_{2}}{V_{p(1)}}\right) = O_{1}M_{1}\left(\frac{M_{1}|W_{2}}{V_{p(1)}}\right) = \frac{M_{1}^{2}(W_{2})}{V_{p(1)}} = \frac{M_{1}|W_{2}}{V_{p(1)}}$ 

So if we want to understand [90] better than whithe
it's more likely that last 2 1/2 or last 4 /2, we
would seem to want to have another copy of 14>
we could measure. We need to run our measurement experiment
on (4) again.
IF we had non copies of 147 at our disposil, we could
do the negarement on all of them. If we did so k thing
then, with high pobelity, we can expect
$  g_0 ^2 - \frac{\# of O outcomes}{k}  \leq O(\frac{1}{\lambda k}).$
This could be made more precise

Take-away: IF we have an unlimited supply of copies of IY?
We can, with high produbility, approximate loold in bainary
reasonably etficiently.
$\frac{1}{1}$
. Maybe there's a better measurement to take.
There's not.
2. What if we don't have no conver of 142?
h/pire SUNK
· · · · · · · · · · · · · · · · · · ·

II. No cloning Soutimes: (07 will men 10) On
In short: there's no unitary way to copy quatur
States.
(hun het n?m. Then there is no unitary trasformation
$V: ( T^{m} \otimes ( T^{n} \rightarrow ) ( T^{m} \otimes ( T^{n} \rightarrow ) )$
such that ((1478/0))= 1478/478/0)
For all 147 E (m.
Proof: There call be, because
14/0/07 F> 14/0/14/0/0)0n-m
is not linear!

		• •	• •		• •		• •		•	• •				• •		• •	• •	• •			 		• •			
			• •		• •		• •														 		• •			
			• •																		 		• •			
			• •																		 					
			• •																		 					
		• •	• •				• •																			
		• •	• •				• •																			
			• •																		 		• •			
		• •	• •				• •																			
			• •				• •																			
			• •																		 		• •			
			• •							• •								• •					• •			
		• •	• •		• •		• •		•	• •				• •		• •	• •						• •		•	
			• •		• •		•							•		•	• •	• •			 		• •			
		• •	• •		• •		• •			•		• •		• •		• •	• •	• •					• •			
		• •	• •		• •		• •			•		• •		• •		• •	• •	• •					• •			
		• •	• •		• •		• •			•		• •		• •		• •	• •	• •					• •			
		• •	• •		• •		• •			•		• •		• •		• •	• •	• •					• •			
	•	• •	• •	•	• •		• •		•	•	•	• •		• •		• •	• •	• •					• •		•	•
	•		• •		• •		•				•		•	•		•	• •	• •			 	•	• •		•	
	•		• •		• •		•				•		•	•		•	• •	• •			 	•	• •		•	
	•		• •		• •		•				•		•	•		•	• •	• •			 	•	• •		•	
•		• •	• •		• •		• •		•			• •		• •		• •	• •				 		• •			
	•		• •		• •		•				•		•	•		•	• •	• •			 	•	• •		•	
	•		• •		• •		•				•		•	•		•	• •	• •			 	•	• •		•	
	•		• •		• •		•				•		•	•		•	• •	• •			 	•	• •		•	
•		• •	• •		• •		• •		•			• •		• •		• •	• •				 		• •			
	•		• •		• •		•				•		•	•		•	• •	• •			 	•	• •		•	
	•		• •		• •		•				•		•	•		•	• •	• •			 	•	• •		•	
	•	• •	• •		•		• •				•			•		• •	• •	• •					• •			
	•	• •	• •		•		• •				•			•		• •	• •	• •					• •			
		•	• •		• •		• •			• •				• •		•	• •	• •					• •			•

· · ·	•	•	•	•	•	•	· ·	•	•	•	•	•	•	•	•	• •	· ·		•	•	•	•	•	•	•	· ·	•	•	•	• •	· ·	•	•	· ·	•	•	•	• •	••••	•	•	•	• •	· ·	•	•	•
• •		S	D D		հ		و		•	r C	ંવ	, , ,	•	•	۲ ۵			.   .	•	r Q	) ຍ	°p	C	•		- 		•	•	Ċ	5		, (	C	he	1-7			V-		e	ſSŢ	fer	למ	ہ ( \ ا	•	• • •
••••		Ś	te	<i>۲</i> ۲	0	>	· ·	ł	h	- - -	$\uparrow$	•		V	२	• •	· ·	{	۲~	- 	<u> </u>	/	•	Ļ	) D	L	•	•	4	2	••••	p	<u>~</u> ~	<i>[</i>	) Qe	רי גיי נ	۲ ۲	•	••••	•	•	•	• •	•	•	•	•
		•	•	•	•	•	••••	•	•	•	•	•	•		•	• •			•	•	•	•	•			•••					• •	•	•		•	•	•			•			• •		•		•
• •			•	•	•	•	• •	0			0	0	•	•		•				•	0	•	•	•	•	• •	0	•	•		• •	•	0	• •	•	•	0	•		•	•	•	• •			0	•
		•	•	•	•	•	• •			•	•	•	•	•	•	• •				•	•	•	•				•	•	•	•	• •	•	•	• •	•	•	•			•	•	•	• •		•		•
• •		0	•	•	•	•	• •	•	•		0	0	•	•		•			•	•	0	•	•	•	•	• •	0		•	•	• •	•		• •	•	•		•		•			• •		•	•	•
• •	•	•	•	•	•	•	• •	•	•	•	•	•	•	•		•			•	•	•	•	•	•	•	• •	•	•	•	•	• •	•	•	• •	•	•	•	•		•	•	•	• •		•	•	•
		•	•	•	•	•	• •	•	•	•	•	•	•			• •			•	•	•	•	•	•			•	•	•	•	• •	•	•	• •	•	•	•			•	•	•	• •		•	•	•
	•	•	•	•	•	•		•	•	•	•	•	•	•		• •			•	•	•	•	•				•	•	•			•	•		•	•	•			•	•	•			•	•	•
		•	•	•	•	•				•	•	•	•	•					•	•	•	•	•	•			•	•	•			•	•		•	•	•			•	•	•			•	•	•
• •							• •															-			•	• •					• •							•		-			• •				
		•			•	•	• •	•			•	•				•					•	•			•	• •	•	•			• •		•	• •			•	•			•		• •			•	•
• •					•		• •																	•		• •		•															• •		•	•	•

II. Distinguishing states, redux
Instead it defermining 14? completely, we might be happy
to have a procedure to distinguish it from all other states
12) (so long as 107 7 eil 14) For some OER).
How night we go about this?
Basic iden From last filme: "prepare" measuremet
$M_{0} = 1475741$ , $M_{1} = I - (24)5741$ .
IF this measurement of (?) ever takes outcome 1, we know
18) is not equal to 147. This procedure works, but
Many issues! Can only get around all at them in special arcumstances

|. Maybe  $|\psi\rangle = a |\psi\rangle + b |\psi\rangle (h|^2 + |b|^2 = 1)$ where (T/v)=0 and 1612 = Jk. Would expect to have to perform the measurement experiment 2th times before we see 187 isn't 1247. L. Just as before: need to have many copies of 14). 3. How do we "prepare the measurement" /247/24/ Would suffice to have a vay to prepare 14), i.e. 9 transformation that takes 107=10-07 to 1247. Can we do batter? IF U: [" -> [" does U/07 = 17], fly 14754187= U147541U5187=10>(01Ut18)

IV. Some good news: Deutsch-Jozsy algorithm
ENDUGH OF THE WARNINGS!
WHAT ARE QUANTUM STATES GOOD FOR?
Duyl to the moral that a guestion state stores
exponentially many classical probabilities (*) we have the philosophy.
ENTANGLEMENT IS
A RESOURCE.
(*): This does NOT mean we can reliably store an exponential quount of classical intormation in a linear # quits (Holevo bound)

Separable US. Entengled states Given a composite quatum system HAR = HA & HB, We say a state is separable if it's of the form  $| \varphi_A \rangle \otimes | \varphi_B \rangle$ For some (PA7EHA, (PB)E)HR. IF 187EHAB is not separable, it is entraped.
Deutsch's Problem
Input: a black box Function
F: {0113 ~>> {0113
which is promised to be either.
i) Constant, or
ii) balanced, meaning $\# F^{-1}(o) = \# F^{-1}(1)$
Problem: Decide Mether F is constant or balanced.
Classically, requires 2"+1 evaluations of F.
· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·

IF we have access to guatur black box function For F, we can solve the problem in Constant time!  $U_{\mathcal{F}}: (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes n} \longrightarrow (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes n}$  $|\chi\rangle \otimes |\chi\rangle \longrightarrow |\chi\rangle \otimes |\chi \otimes |\chi \otimes f(x)\rangle$ Boolean addition ancilla quests of bit strings TL: flips Y' = Trst(7) L: t it <math>F(x) = 1 or does nothing T(x) = 0. 

Details (Nielsen - (hung)

## Algorithm: Deutsch-Jozsa

**Inputs:** (1) A black box  $U_f$  which performs the transformation  $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ , for  $x \in \{0, \ldots, 2^n - 1\}$  and  $f(x) \in \{0, 1\}$ . It is promised that f(x) is either *constant* for all values of x, or else f(x) is *balanced*, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half.

Outputs: 0 if and only if f is constant.

Runtime: One evaluation of  $U_f$ . Always succeeds.

Procedure:

1. 
$$|0\rangle^{\otimes n}|1\rangle$$
 Q  $\sqrt{7}$  aging Since  
2.  $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$   
3.  $\rightarrow \sum_x (-1)^{f(x)} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$   
4.  $\rightarrow \sum_x \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$   
5.  $\rightarrow z$ 

initialize state

create superposition using Hadamard gates

calculate function f using  $U_f$ 

perform Hadamard transform

measure to obtain final output z

	<u>C</u>	<u>a</u>	/ <del>८</del>	<u>-</u>	5			•	• •		•				•••	•		•	• •		•		•		• •	•			•	• •			•		• •	•	· ·	•
•	. (.		С	0 0	tri	VP	J	0	p c	-D	)e e	5						0	• •		•	• •	•	• •	• •	0			0	• •	o o				• •	0	• •	•
•	5	ļ.	$\sum$	حا	<u>ئ</u>	.cl	1 1		P	، د ۲	Ы	eV	<b>7</b>	C	, an		P	٩	e	开		ien	J.).	-J	5	 	Ve	2	. \	vi	ļι	n.	•	•	• •		• •	•
•	• •		h	 ເອັ	<b>2</b>		، م ر	ļ	2	ぴ	1	1-	4		57			1	C	10	15.	ים ריים ריים	-	í	, .		-96	n'l	: ;-{	'כ	• •	•	•	0	• •	0	• •	•
•	· ·	•••	( <b>1</b>	, <b>L</b>	∩∦P		fe	- <sup>1</sup>	• •	ر مرابع	ب ت	وم		<b>.</b>	) 1	:t	لسو	•	ماو	700	.1	م م لم	•	( a	1 1	Ŧ	م: ا	, . , . , .	, ,	ົວ	ึ่า	S_		•	• •	•	• •	•
•		δ ζ.	ļ	py	) )	S		2	J 1	, D	, , ,	م س	pe !	5		Ĺ	> -	nc/	<	6	و م	יי גיי ג	د	/\$,	•	, 1	ەپ	Ĵ	- Un	<b>n</b>	L	,/q	10	h	L	אס	יי אי נ	•
				· • · •							•							•	• •	• •		• •			• •					• •	• •	•	•				• •	
	• •						• •					•										•									• •				• •	•	• •	
								•		•	•	• •		•		•		•	• •	• •	•	• •		• •	• •	0			•		• •	•	•					
	•		•	• •		• •		•	• •	•	•	• •		• •	• •	0			• •	· ·	•	• •	•	• •	• •	•	• •			• •	0 0 0 0	0	•	•	• •			•
	• •		•	• •		· ·	• •	•	• •	•	•	• •		• •	· ·		· ·	•	• • • •	• •	•	· ·	•	• • • •	· ·	•	• •	· · ·	•	• •	• •	0	•	•	• •	•	• •	•
•	• •		•	· ·		· · ·	· · ·	•	· · ·	•	•	• •				•	· · ·	•	· · ·	· · ·	•	· · ·	•	· ·	•	•	• •		•	• •		•	•	•	· ·	•	· ·	0
•	· ·		•	· · ·			· · ·	• • • •	· · ·	•	•	· · ·				•		•	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	•	· · · · · · · · · · · · · · · · · · ·	• • • •	· · ·	· · ·	•	• •		•	· · ·	· · · · · · · · · · · · · · · · · · ·	•	•	•	· · ·	•	· · ·	•
•	· · ·		•	· · · · · · · · · · · · · · · · · · ·			· · ·	•	· · ·	•	•	· · ·				•		•		· · · · · · · · · · · · · · · · · · ·	•	· · · · · · · · · · · · · · · · · · ·	· · ·		· · ·	• • • • •			•	· · ·		•	•	•	· · ·	•	· · · · · · · · · · · · · · · · · · ·	•
•	· · ·		•	· · · · · · · · · · · · · · · · · · ·			· · ·	•			•					•		•		· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·							•			•		•	· · · · · · · · · · · · · · · · · · ·	•	· · · · · · · · · · · · · · · · · · ·	•
•	· · · · · · · · · · · · · · · · · · ·		· · · ·	· ·							•					· · · ·		•		· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·	· · · ·						•					· · ·	· · · · · · · · · · · · · · · · · · ·	• • • • • •	· · · · · · · · · · · · · · · · · · ·	
•	· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·													- - - - - - - -		• • • • • • • • • •		· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·								· · · · · · · · · · · · · · · · · · ·				· · · ·	· · · · · · · · · · · · · · · · · · ·	· · · ·	· · · · · · · · · · · · · · · · · · ·	
			- - - - - - - - -									· · · · · · · · · · · · · · · · · · ·									• • • • • • • • • •	· · · · · · · · · · · · · · · · · · ·			· · · · · · · · · · · · · · · · · ·					· · · · · · · · · · · · · · · · · · ·						• • • • • • •		

Meeting 6.1. I. Probabilis II. Reversible	: Classical warm ups to quatum computing tic classical computing: BPD and MA classical computing
Next time:	quantum circuits, BRP and RMA
	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
	· · · · · · · · · · · · · · · · · · ·
	· · · · · · · · · · · · · · · · · · ·

Axioms of quantum mechanics lead to important problems it we want to use quatum mechanical systems to build a computer, even in the ideal case of a noise-less system: 1. The classical information extracted via measurement is a probability distribution. Hav Can we formalize complexity theory around this? J. IF we want to use a Hilbert space of some system as a "quantum memory register," then (quantum) transformations must be unitary, hence, in particular, invertible/ reversible. Is reversible computation fegsible?

Goal today: answer these questions in classical
Warm-up Cases.
The classical analogs won't address all of the issues in the quantum case. E.g. quantum stortes are not just' classical probability distributions, and unitary group U(1) is Uncountably intircte.
Also important loter: non-ideolized quartur computing. Need a theory of quantum error corrections and Fault tolerance.

I. Pr-babilistic classical computing
Informally: a classical probabilistic algorithm is any algorithm
that is allowed access to tain flips, or, equivalently,
randown bit strings
Two equivalent ways to make this more Formali
1. Extend the definition of Turing machine so the transition
Function can, in addition to using the machin's internal
State and read of the memory, toss a fair coin.
2. Resolve a non-deterministic Turing machine by Flipping
a coin to decide how to branch.
· · · · · · · · · · · · · · · · · · ·

Remarks:
1. It doesn't matter so much if the coin is fair, but if
p(heads) = 1/2, it should at least be a reasonable number
2. Coin tosses are always independent. So our algorithm could
do all of them at the beginning. Equivalent to choosing
a (uniformly) random bit string, and using the bits one
by one as needed.
3. Access to coin tosses doos not change "competable."
It might change "etticiently computable", thus violating
extended Church-Turing thesis.
4. Flipping a coin courts as one time step.
· · · · · · · · · · · · · · · · · · ·

A probabilistic algorithm / Turing machine For a Counting
problem induces, for any input X, a probability distribution on {0,1}*.
For a decision problem, each input x yields 9 problem/ $H_{\gamma}$ distribution on $\{0,1\} = \{Yes, No\}$ .
Intermally: A decision protien should be considered etficiently
probabilistically solvable if there's a poly. time luring machine that get's the correct assurer with high probability.

Fix a constant $0 \le \le 1/2$ . A decision problem L is in BPP <sub>E</sub> ("bounded-error probabilistic polynomial time") it there exists a PTM T and a polynomial $p(1x)$ such that when input x, T terminates in at most $p(1x)$ steps,
and: (i) $t \in L(x) = Yes, then T assures Yes w/ probe Z = 1-\varepsilon > \frac{1}{2}.(ii) t \in L(x) = No, then T assures No w/ probe Z = 1-\varepsilon > \frac{1}{2}.$
Sol E is probability of a wrong answer.

Fact: For any OLELE'L 1/21	· · · · · ·
$BPP_{\varepsilon} = BPP_{\varepsilon'}$ .	· · · · · ·
Why? "Amplification of probability." BPPE E BPPE/ Obvious from detinition R PD > RPP : const (const. (const. ) - d	· · · · · · · ·
DFFE = DIFE / repear (enough times) and use majority (ull.	· · · · · · ·
Take-away: DeFine BPA = BPP1/3'	· · · · · · ·
Equivalent Formulation: BPP is all decision problems L decidable on NA TM such that at most 1/3 of the branches cepart the wrong assures.	8 <sub>7</sub>

Variats: RP, PP	
RP: some as BPP, except if the assure is	Yos, the
T 100 givens reports the correct ensuel.	· · · · · · · · · · · · · · · · ·
PP: what we get iF we set E=1/2	· · · · · · · · · · · · · · · · ·
BPPo = P. (But bourse of ZPA)	
	· · · · · · · · · · · · · · · ·

Example: Pr;	mality testing	is in BP	P Vig	
Miller - Robin	test.	· · · · · · · · · · · · · · ·	· · · · · · · · ·	
Input: inatur	al your for	N (n b	mary)	· · · · · · · · · · · · · · ·
Question: 15	N prim	e?		
· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · ·	· · · · · · · · ·	
In Fact,	17 W 55	shown	70 E	e ا
ín	P.			
· · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · · · · · ·

<u>Deradomization</u>: It's expected good random number generators exist, have BPP=P.

Merlin-Arthur: probabilistic analog of NP. Has some detinition as before, except we use a BPP Turing machine to decide when a witness is believable
Nome Merlin-Arthur is supposed to invoke a gome.
Multi-round (but constant) games generalize NP (or MA)
to polynonial hearing.
· · · · · · · • · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·

I. Reversible classical computing
Classically, interested in computing Boolean Functions
f: {0,1}3 <sup>m</sup> → {0,13 <sup>n</sup>
OF course, these are not all bijections. Is there a may
to encode F "inside" of a bijection?
Even better, can we do this "locally" and "any formaly"?
$\Gamma_{1}$
$\Gamma$ rest $C$ $A$ $I$ .
Mistary: Boolean circuit C
Prist CSAI. Instance: Boolean circuit C Question: Is C satisfiable?
Mistarce: Boolean circuit C Question: Is C satisfiable?
Mistore: Boolean circuit C Question: Is C satisfiable?

Booleon circuit ic Something like this! Placer \$0,1} = {Ya,No} Drawn Vror ontes plane Who classings of where AND bring NOT Noil A' ND  $\bigcirc$ (0,1,1,0,1) = 1, sois satisfiable

· · ·	7	We	h	<b>∍</b> √ℓ	· · · (	- ^ ° ?	s Sra	gs,	· · ·	ja	7	يح	Ì		îd	) .	~//		<b>7</b>	ی		70	•	· ·	• •	•	•
• •	• •	· · · ·	• •	• • •	• •	• •	• • •	• • •	• •		• •	• •	• •		• •	• •	• •	• •	• •		• •	• •	•	• •	• •	•	•
• •	• •	· · · ·	• •	• • •	• •	• •	• • •	• • •	• •			• •	• •		• •	• •	• •	• •	• •		• •	• •	•	• •	• •	•	•
• •	• •				• •				• •		• •	 . 1		1	• •	• •	•••	• •	•••	•	•••	•••	•	•••	••••	•	•
	o o						• • •	• • •			• •		0 0									•••			••••		•
· ·	• •	· · · ·	• •			• •	· · ·				••••	5		AF	/ د ا	· ·	· ·	· ·	· ·	•	· ·	•••	•	· ·	· ·	•	•
• •	• •	• • • •		A	R		• • •		• •	• •		1	f			• •	• •	• •	• •	•	• •	• •	•	• •	• •		•
• •	• •			• • •				• • •	• •						• •	• •	• •	• •	• •		• •	• •	•	• •	• •	•	
• •	• •	· · · ·		· · ·	• •	• •	· · ·	· · ·	• •		••••		• •		• •	• •	• •	• •	• •		• •	• •		• •	• •	•	•
• •	• •			••••	• •	• •	• • •		• •		• •		• •		• •	• •	• •	• •	• •		• •	• •	•	• •	• •		•
	• •		• •		• •	• •	- • •		• 0 0 0		• •	• •	• •		- v 0 0	- • • •	- ×	- • 0 0	· 0	0	- v 0 0	- 0 0 0	0	- • • •	· 0	•	
• •	• •	· · · ·	• •	· · ·	• •	• •	· · ·	· · ·	• •		• •	• •	• •	• •	o o o o	• •	• •	• •	• •	0	• •	• •	•	• •	• •	•	•

CSAT (Con red	is NP-comple uce From SAT!	ete.		
Size of	9 circuit is $O(\#$	gates).	· · · · · · · · · ·	
ls there reversible	some NA-complete circuits?	analog of C	s#7 †	\$ \$
· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	 	.       .
· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·			
			· · · · · · · ·	
· · · · · · · · · · · · · · · ·			·       ·	

Fix a gotte set &, which a set of hijections q: {0113" -> {0,13" where a may vory with the gate. We can use gates from 29 to build planar reversible circuits. 94 11 33 g; EL 91 32 width 5 711 12  $\mathbb{R}: \{0,1\}^{S} \longrightarrow \{0,1\}^{S}.$ 

Q: Con ve Find on NP-complete problem For circuits with gate set g? Call it RSAT (2) ---A: Depends on D. Why is this unclea? Note, we con't Fix  $y \in \{0, 1\}^n$  and as in the exists  $x \in \{0, 1\}^n$  such that R(x) = y? Why not? Because the assure is shorys Yes!

Let	2 = Sym ( 20,133), and define RSAT(2)
as f	Blows:
Input:	Reversible circuit R of width 2K
Quecton :	Dees thre exist xiye {011} K such that
· · · · · · · · · ·	$R(x_1, 0,, 0) = (y_1, 0,, 0)$ ?
· · · · · · · · · · · · · · · · · · ·	k lk
( <u>[</u> ].	This is NP-complete
· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·

Meeting 6.2 T. RSAT	: Reversible	Computing	and quantum	circuits
I. Quantum	circuits	· · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · ·
Next time:	Solovay - Kit	aev?	· · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · ·		· · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · ·		· · · · · · · · · · ·		· · · · · · · · · · · · · · · · · ·
·       ·		· · · · · · · · · · · ·		.       .
.       .		· · · · · · · · · · ·		·       ·
			.       .	

I. RSAT Last time: 9 (Boolean) gate set & is a set of bijections  $\{0,1\}^{k} \rightarrow \{0,1\}^{k}$ (K Varieble) A planar, reversible Boolean circuit R is a diagram like +6,1 94 R encodes a function R: {0,1}" -> {0,1}"  $\left| \left( \begin{array}{c} \frac{1}{3} \\ \frac{1}{3} \end{array} \right) \right|_{q_{i}} \in \mathcal{L}$ The circuit is q 9, 3, 3, 1 171 11 11 15 "planar &- Factorization of this function. depth: 3

Note: every Boolen Function (not necessarily reversible)
$f: \{0,1\}^m \longrightarrow \{0,1\}^n \xrightarrow{\times} \{0,1\}^n$
can be built out of AND, OR, ad NOT, FANOUT
{AND, DR, NOT} is a Universal set of logic gastes.
If we want to Find interesting computational problems for
reversible circuits, & better he sufficiently rich."
· · · · · · · · · · · · · · · · · · ·
Lots of viggle
Lots of Viggle room!



· · ·	•	(	- ) (	`ບ ເ	2	•	· · ·	2		· · ·	•	•	g	• • •	•	{	D	)		ر کے	k	-		7			9	12	), }		•	•	• •	•	•	•	· · ·	•	•	· · ·
• •		C	a	0 0	al		مرابع	s .	L						(			]	•		י ה/פ	•	0	, ( ,	(		501	$tr_{z}$		le	J				·)		 0 0			• •
• •		• •			•										•	•		• •	•			•	•			•		• •	•	• •					•				•	
• •		• •		• •	٠		• •			• •								• •			• •			•	• •			• •		• •			• •		•		• •			• •
• •				• •						• •																				• •										
• •		• •		• •			• •		•				•	• •							• •				• •			• •		• •			• •				• •			• •
• •	•	• •		• •			• •		•	• •				• •			•			•	• •			•	• •			• •		• •	•		• •			•	• •			• •
• •				• •																										• •										
• •		• •		• •			• •			• •				• •			•	• •			• •				• •					• •			• •				• •			• •
• •	•	• •		• •			•		•	• •				• •			•				• •				•		•			• •			• •		•		•			• •
• •		• •		• •						• •				• •			•	• •			• •				• •			• •		• •			• •				• •			• •
• •		• •		• •													•								• •					• •			• •				• •			
• •		• •		• •			• •			• •							•				• •			•	• •			• •		• •			• •				• •			• •
• •		• •		• •		•	• •			• •				• •			•				• •				• •			• •		• •			• •				• •			• •
• •		• •		•			• •			• •				• •				• •	-		• •		-		• •			• •		• •			• •				• •			•

st for Fun: Since t is Conservature 156

Figure 3.14. A simple billiard ball computer, with three input bits and three output bits, shown entering on the left and leaving on the right, respectively. The presence or absence of a billiard ball indicates a 1 or a 0, respectively. Empty circles illustrate potential paths due to collisions. This particular computer implements the Fredkin classifier reversible logic gate, discussed in the text.

we can implement it with billiard balls

Figure 3.16. Fredkin gate configured to perform the elementary gates AND (left), NOT (middle), and a primitive routing function, the CROSSOVER (right). The middle gate also serves to perform the FANOUT operation, since it produces two copies of x at the output. Note that each of these configurations requires the use of extra 'ancilla' bits prepared in standard states – for example, the 0 input on the first line of the AND gate – and in general the output contains 'garbage' not needed for the remainder of the computation.

T

T

If we allow extra "ancilla" toits, can encode AND, OR, NOT:

AND (XIT)

xy

 $\bar{x}y$ 

x

ee

ine

ply

tive

()

r



CROJSOUER,

SWAP

Recall: De Morgan XUY = - (-X1-Y) NOT NOT [ No, ]

Since NOT and SWAP are reversible, might as well include them in 2 For your  $\mathcal{L} = \{F, NOT, SWAP\}$  $(1^{+} \longrightarrow (1^{+} \otimes 1^{+})) \otimes (1^{+} \otimes 1^{+})$  $\times$  is a  $\longrightarrow$  in  $\times$  in  $\times$  in  $\otimes$  in  $\times$  in is not linear!

We can "dilate" every Boolean circuit to a revusible Circuit, by replacing every AND with a Fredhin + ancillae in O state: dilate AND AND FINOT

RSAT (	E), Variant 1:	&={F, s~A	r, Not}.
Instance:	reversible (planar) & - cir	cuit R, with inpu	4
· · · · · · · · · · · · · · ·	divided into donta cegiste	r of width d	
	and ancilla register of width(R)=4, and all anc	illae set to D.	· · · · · · · · ·
Pr-blen:	Does there exist $x \in \{0\}$ the first output bit of	R(X, 0,, 0) is	J?
Lemma: RS	AT(2) is NP-complete.	<b>ルー</b> プ	
<u>Proof</u> : Reduc	e from CSAT Using dil	ation os on previous	poge. D

of some what	less contrived Variat	, we can build t of RSAT.
Here COPY	ίς.	
.         .	$ \begin{array}{c} X \oplus Y \\ \int \\ \int \\ C D P Y \\ \hline \\ Y \\ Y \end{array} $	COPY is "Teversible copy" not "cbre" or "Fan out" x x [] [ [ Farout]
(17 x=0, C	OPY Copies y to	×.)
2 = {	F, SWAP, NOT, C	σβγξ

RSAT (	ED, Voriant 2:
Instance:	H-circuit R with vith (R) = 2n, with input
· · · · · · · · · · · ·	divided into data and ancillae registers both
	of width n.
Problem	Do there exist xig E {0,1}" such that
· · · · · · · · · ·	R(x, 0,, 0) = (y, 0,, 0)
· · · · · · · · · · ·	ancillae ancillae
· · · · · · · · · · ·	
Lening.	(his problem is NP-complete.
· · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
Prof: Key iden is Uncomputation, which is also useful in quantum computation ad in complexity cesults in topology. See "Computational complexity and S-manifolds and Zombies by Kuperberg-S.) leduce from First vorient. Three coses Not(ril) XI .... Xn 91, 91 Yi Yn bi big I... I ... I of R.I Three coses Not(ril) XI .... Xn 91, 91 I... I I R and apply 9 NOT XI X n ak 9k+1 X, X, n 9k Case :: 1= k+1 Mne ancilla

Case it 47 K+1 . . .... Inh, DK NOT uncompute Copy and pad v/ new ancillae XI X 91 9K 9k X X N 9k 9k129 Several more Padding Dc://g (cgister

Case jii n 4 Ktl COPI-Con Xn 9, X۱ Nor 1 Nor' and pro COPT ----|-...|···` . ~ .\_ - .  $\mathbf{X}_{i} = \mathbf{X}_{i}$ 91 · X New INAVT The copying at the end is to a parsimonious rediction. ensure

W4-1 U1	ncomputation is releva	It to quartures computing.	•
We m.	ight work hand to p	prepare quarture state (7)	•
So w	e can do Usotul fli	rgs with it.	•
· · · · · · · · · ·			•
[v]	~[~~]	Potertiolly - Image Cise matative 1	•
	$\cup$ $\Box$ $\Box$ $\Box$	Output might Lo	•
	_ junk?	Critoraled w/ 41	•
	$2^{k}$	junk 1	•
	$z_{i} c_{1}(1)$ $i \ge 0$		•
			•
			•

Interesting question:
Given jote set &, whyt's the
complexity of RSAT (8)?
le: "How powerful is 2?"
$\sim$
Quess: Either its in P
or its NP-complete?
(See Schaeter dichotomy theorem)

<u>II. (</u>	Quant	ŪM	<u>(</u> :	rcuit <u>e</u>		· · ·	· · ·	· · · · ·	· · · ·	· · ·	· · · ·	· · · ·	· ·	· ·	· ·	· · · ·
Cal		Cu	<i>it</i> er	$\gamma$	frasti	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	<i>†</i> !e-1	· · · · ·	· · · ·	· · ·	· · ·	· · ·	· ·	· ·	· ·	· · · ·
· · · · · · ·	J	):		©	⊗ (° ~`		♪ ((	<u>)</u> ~ 8	) (			· · · ·	· ·	· ·	· · ·	· · · ·
· · · · · · · · ·				k		· · · ·	· · ·	· · · · ·	· · · ·	· · · ·	· · ·	· · · ·	· ·	· ·	• •	· · · ·
Any	n-ar set	7 ¥	gua,	9conte	ן <i>ם</i> זאן קאי	tes		Cylle	d d	2 2	nte	7 5 5 5	J.	· ·	· ·	· · · ·
· · · · <b>/</b> · · · · · · · · ·		· · · · ·	· · · · ·	<b>+</b> • • • • • • • • • • • • • • • • • • •		· · · ·	· · ·	· · · · ·	· · ·	<b>∧</b>  	· · · ·	· · ·	· ·	• •	· ·	· · · ·
· · · · · · ·	· · · · ·			· · · · ·	· · · · ·	· · ·	· · ·	· · · · ·	· · ·	· · ·	· · ·	· · ·	• •	• •	• •	· · ·
· · · · · · ·	· · · · ·	· · · · ·	· · · · ·				• • •	· · · ·	• • •	• • •	· · ·	· · ·	• •	• •	• •	· · ·
													0 0	• •	•	

Any classical reversible	gale a	( cm	be	line		· · ·	• •	· · ·	• •
(F a: 50,13 K ->	Son k	· · · ·				· · ·	• •	· · ·	
(×₁,,× <sub>k</sub> )⊢	⇒ (Yı Yk)			· · · · · ·		· · ·	• •	· · ·	
The						• • •	• •	• • •	• •
(~~~)	17W7	· · · ·	• • •	· · · · · ·	· · · ·	• • •	• •	· · ·	• •
		· · · ·	· · ·	· · · · · ·	· · · · ·	· · ·	• •	· · ·	• •
<u> </u>		· · · ·					• •	••••	• •
· · · · · · · · · · · · · · · · · · ·			• • •			• • •			
The quarter gute g	pernetes	fle	Com	putation	nal 6	C12.3	· · ·	· · · ·	· ·
of ((1)) Take-avo	guatram	Cr CV	its a	include	c (-15 ic	ମ	• •	· · ·	• •

2. Line	CNOT of	(9Kg COPY) CNOT			
	CNOT -	{0,132 - 00 01 H 10	{01} 00 01 11	<td> </td>	
<td></td> <td></td> <td>10 1×c=y&gt;</td> <td>/y&gt; 1</td> <td> </td>			10 1×c=y>	/y> 1	
	C NOT        X7 (47		[*) [·	7 r>	

3. Single qubit gates pir untage portos on Office
Hadamand LI - 1 / 1 1) Lie group U(d).
$\frac{1}{\sqrt{2}} \left( 1 - \frac{1}{2} \right)$
$\sim$
Physe gostes: 11 [iv] / 10]
$\left[ \underbrace{e}_{\mathbf{r}} \right]^{2} \left( \begin{array}{c} 0 \\ e^{i \Psi} \end{array} \right)   \times /$
A 9/0>+5/12 1-> 9/0>+, ile,
$ x\rangle$
· · · · · · · · · · · · · · · · · · ·

A quatur circuit over & is a circuit whose gates
gre elements of 2.
Just as for classical reversible circuits, quatury
circuits have a width and a depth.
E.g. C implements a unitary
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
$C: \begin{array}{c} X \\ \uparrow \end{array} \\ \uparrow \end{array} \\ \begin{array}{c} X \\ \downarrow \end{array} \\ \begin{array}{c} X \\ \otimes C \\ N \\ O \\ \end{array} \\ \begin{array}{c} X \\ \otimes C \\ O \\ \end{array} \\ \begin{array}{c} X \\ \otimes C \\ O \\ \end{array} \\ \begin{array}{c} X \\ \otimes C \\ O \\ \end{array} \\ \begin{array}{c} X \\ \otimes C \\ O \\ \end{array} \\ \begin{array}{c} X \\ \otimes C \\ O \\ \end{array} \\ \begin{array}{c} X \\ \otimes C \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \begin{array}{c} X \\ \otimes C \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} X \\ \end{array} \\$
$\left[\begin{array}{c} c N o T \\ h \end{array}\right] \left[\begin{array}{c} e^{i \varphi} \\ f \end{array}\right] 1^{2}$
depth: 2 w. dth: 3

Gate set & is precisely if (for a large enough)
every unitary $U: (\mathbb{C}^2)^{\otimes n} \rightarrow (\mathbb{C}^2)^{\otimes n}$ can be expressed
as a 21-circuit. (Every UEU(2n) can be factured as a product of elements of 21.)
U(2) + CNOT is Universal quatum gate set.
(n fact: phase gates + H + CNOT is universal.
"Precisely universal" is overkill!
Why? Quatum computers are probabilistic and
states that are too close can not be feasibly
distingvished.

A better definition (but still orguably overkill...) A grie 21 is (plann) quatum universal if for all 4 lage enough, elements of & in  $\mathcal{U}(\mathcal{L}^{2}\otimes\cdots\otimes\mathcal{L}^{2})\cong\mathcal{U}(\mathcal{L}^{n})$ (ie, given gED that is binny, we get und differt Unitaries of the form 10(2)@i & g & 10(C2)m-2-i) genurate (as a monoid) à derse subset (For all 270 For every UCU(25), we can find a Sincevit U' s.t. IV-U'II 4 E.)

Let F: be q precision 2 <sup>m</sup> - 2 2 2 2 2 2 2 2 2 2 2 2 2	$\{0,1\}^{n} = Font:on.$ $\varepsilon$ $\{(x), z\}$	$= \frac{1}{20}, 13^{m}$ $A  C:CCUTF$ $O \leq \varepsilon \leq 1/2$ $\int \bigcup \left( x, 0^{N} \right)$	U <u>comput</u> if for any -n>1 2 1-	e> F f= ×ε ξ0113" ε.
· · · · · · · · · · · · ·	· · · · · · · · ·	00	· · · · · · · · · · · · ·	
(V 4-5	width N	)	· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·

I. BQP, gote (in)dependence, and the Solovay-Kitaer theorem Last time, I ended by Flacking this definition (taken from the fextbook of Kitner et al.):
Let $F: \{0,1\}^n \longrightarrow \{0,1\}^m$ be a function. A circuit () computer $F$ to precision $\mathcal{E}$ ( $0 \leq \mathcal{E} \leq 1/2$ ) if for any $X \in \{0,1\}^n$
$\sum_{z=0}^{2^{N-m}} \left  \left\langle F(x), z \right  \left( 1, 0^{N-m} \right) \right _{T}^{2} \geq 1 - \varepsilon.$ $Forget last time$
(U has width N)

· · · · · · · · · ·		· · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
$\mathbb{V}$ L	، (	+his	9	g oo d	.       .
· · · · · · · · · ·	definit	tion?	  		.       .
	Convenience,	٩٢٥٥٩	<i>[</i> , , , , , , , , , , , , , , , , , , ,	÷ ),	
· · · · · · · · · ·			· · · · · · · ·	· · · · · · · · ·	
· · · · · · · · · ·		· · · · · · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · ·		.       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .	· · · · · · · ·		· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·

Do measurement
$M_0 =  O  \langle O  \otimes  O  = M_1 =  I  \langle I  \otimes  O  = On$
Ulx, ON-n). Probability of correct outcome f(x) is
$\langle x, O^{N-n}   U^{t} M^{t} M U   x, O^{N-n} \rangle$
$W_{r:te}$
$\bigcup[x_1 o] = [+(x)] \bigotimes (\sum_{z} c_{z} (z)) + [+(x)] \bigotimes (\sum_{z} d_{z} (z))$ $\frac{1}{z}$
where $\sum_{2}^{7} (c_{2})^{1} +  J_{2} ^{2} =  .$ Then
$M_{f(x)}U(x,0) = [f(x)] \otimes \sum_{n-m} c_{2}/2), s_{0}$
$P(\text{outcome } f(x)) = \sum_{z=0}^{\infty} \left  \left\langle F(x), z \right  \bigcup \left( x, O^{N-n} \right) \right ^2 \ge 1 - \varepsilon.$

lntu	ition:	• • •	· · · · ·	· · ·	· · ·	· · · · ·	· · · · ·	· · ·	· · · · ·	· · · ·	· · ·	· · ·	· · ·	· ·	· ·	· ·
$\bigcup$	Co	γp	s to s	· · ·	F	;F	· · · · ·	for	م (	×	<b>)</b>	· · · ·	· · · ·	· · ·	· · ·	· · ·
	J [ X		) <sup>N -</sup>	$\sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{i=1}^{n} \sum_{i=1}^{n} \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{i=1}^{n} \sum_{i$	· · · · ·	· · · · · · · · · · · · · · · · · · ·		55e		· · · ·	9 1	· · · ·	· · · ·	· ·	· ·	· ·
State	2		the	• • • •	Foru	· · · · ·	)/F(	(×)) (	ی ( زی-	47	· · · ·	· · ·	· · ·	· ·	· ·	· ·
· · · · · · ·	· · · · ·	· · ·	· · · · ·	· · ·	· · ·	· · · · ·	· · · ·	· · ·	· · · · ·	· · ·	· · ·	· · ·	· · ·	• •	• •	• •
· · · · · · ·	· · · ·	· · ·		· · ·	· · ·	· · · · ·		· · ·	· · · · ·	· · ·	· · ·	· · ·	· · ·	• •	• •	· ·
· · · · · · ·	· · · · ·	· · · ·	· · · · ·	· · · ·	· · ·	· · · · ·	· · · · ·	· · ·	· · · · ·	· · ·	· · ·	· · · ·	· · · ·	· ·	· ·	· ·
	· · · · ·	· · ·	· · · · ·	· · · ·	· · ·	· · · · ·		· · ·	· · · · ·	· · · ·	· · ·	· · ·	· · ·	· ·	• •	· ·
	· · · · ·	· · ·	· · · · ·		· · ·	· · · · ·	· · · · ·	· · · ·	· · · · ·			· · ·			• •	• •

Here's another fair definition:
U computes F to precision E if for any XE {0,13"
$\langle F(x), x, 0^{N-n-n}   U   x, 0^{N-n} \rangle \geq 1-\varepsilon$
Claim Two definitions are equivalent. (E's differ, but by
<u>Proof</u> : For convenience, assume m=).
(1) => (2): Use uncomputation. IF U satisfies
$\gamma^{N-m}$
$\sum_{\gamma=0}^{d} \left  \left\langle F(x), 2 \right  \bigcup \left( x, 0^{N-\eta} \right) \right ^2 \ge \left  -\varepsilon \right .$
then build circuit V as follows:

4 - -()-1 (NOT . . . . . X~O O X  $\mathcal{D}$ N-n (b) => (1): Immediate From detritions.

What should be the correct definition of what it
means for a quations computer to compute a decision problem
F: {0,1]* -> {0,1} = {No, Yes}?
Issue: now input bit string has variable + unbounded length.
Fix: Use a different circuit for every bit string, or
at least every different length n=/x/.
But careful! Where should these circuits come From?
A classical polynomial time
A classical polynomial time algorithm!

$\underline{D_{e}F'_{n}}$ [BQP( $\mathcal{B}, \varepsilon$ )]								
Fix a quantum universal gate set 21 and BLEL 1/2.								
A decision problem f: {0,1}* -> {0,1} = {No, Yer } is in								
BQP(Z, E); F there exists a classical, polynomial time								
algorithm that when input XE{011}*, prints a diagram								
of a quantum circuit (u/gate set 2) Ux that								
of a quantum circuit (u/gate set 2) Ux that Computes F(x) to precision E.								
of a quantum circuit ( $u/gate$ set Z) $U_X$ that Computes $F(X)$ to precision $E$ .								
of a quantum circuit (w/gate set &) Ux that Computes F(x) to precision E.								
of a quantum circuit (w/gate set 2) $U_X$ that Computes $F(x)$ to precision $E$ .								
of a quantum circuit (u/gate set 21) Ux that Computes F(X) to precision E.								
of a guartum circuit (u/gate set 21) Ux that Computes F(x) to precision E.								
of a quantum circuit (w/gate set 2) Ux that Computes F(x) to precision E.								
of a quantum circuit (w/gate set 2) Ux that Computes F(X) to precision E.								
of a quantum circuit (w/gate set 2) Ux that Computes F(x) to precision E.								
of a quantum circuit (w/goite set 2) Ux that Computes F(x) to precision E.								

Dependence on 21 and E?
Just as For BPP, we have
$BQP(\mathcal{B}, \varepsilon_{1}) = BQP(\mathcal{B}, \varepsilon_{2})$
For all $0^{4} \varepsilon_{1} c \varepsilon_{2} c''_{2}$ .
For &, have to consider conversive properties
of dense subgroups of U(2) and U(4).
Problem: need to convert gates in 21, to
gates in & without too much overhead.
Moreover, the conversion is only APPROXIMATE.
· · · · · · · · · · · · · · · · · · ·

Theorem A3.1: (Solovay–Kitaev theorem) Let $\mathcal{G}$ be a finite set of elements in SU containing its own inverses, such that $\langle \mathcal{G} \rangle$ is dense in $SU(2)$ . Let $\epsilon > 0$ be given that $\mathcal{G}_l$ is an $\epsilon$ -net in $SU(2)$ for $l = O(\log^c(1/\epsilon))$ , where $c \approx 4$ .	U(2) iven.
In other words, if GESU(d), I can find	
$U = G_1 G_2 G_2 \cdots G_{l}$ , $G_i \in \mathcal{L}$	· · · · · · · · · · ·
Such that (Assuring	L, and
$\  U - G \  \leq \varepsilon$	sthe towith
where $l = O(\log^{c}(1/\epsilon))$ .	closed,)
Take-away: it's easy to Find a short product .	of )
eleveris of 21 that is E-close to G.	
Corolly; BQP(2,)=BQP(2)	

Warning: if & is infinite, BQP(25) Can include un computable Functions Def BQP = BQP(&, 1/3) where & is whatever Finite, inverse closed, quantum universal gate set you prefer.

Examples of problems in BQP?	• •
Factoring!	· ·
Give an integer on (in binary), out put	· ·
its prime Factorization.	• •
Note: Factoring is NOT the some as	· ·
Is it prime?	· ·
Zarendy in P.	· ·
	••••

I. QMA and local Hamiltonian problem
Kitger's book colls QMA "BQNA"
Three way malogy:
P:NP:: BPP:MA:: BQP:QMA
1. Arthur has a quature computer!
Unité is very similar to mity with two goditions: 1. Arthur has a quature computer! 2. Merlin provides Arthur with a certificate in the
UNIA is Very similar to MA, with two goditions: 1. Arthur has a quature computer! 2. Merlin provides Arthur with a certificate in the Form of a quature state
Unité is Very sandor to Mity with two goditions: 1. Arthur has a quature computer! 2. Merlin provides Arthur with a certificate in the Form of a quature state
Unité is very somilar to Mity with two goditions: 1. Arthur has a quature computer! 2. Merlin provides Arthur with a certificate in the Form of a quature state

Subtlety: it's possible Merlin only ever needs to use a classical bit string. It would be better to call QMA (QMQA) Then there is 7 subset "CMQA" Unfortunately CMQA is actually called QCMA.

			• •		• •					• •					• •					• •										• •			• •		
		· †						1				T			• •	(•			•			1				•		• •		• •					
			S-	•	$\mathcal{N}$	l e	r		iη		6	<u>_</u>  e	15	51	67	).	0	) (	.9	$\mathcal{O}$	ናብ	1.	V	-	5					• •					
																			.7						-										
																														. ,					
																																			-
			• •																																
																												• •							
•	•		• •	•															•									• •					• •		
															• •											•		• •		• •			• •		
															• •													• •					• •		
•	•		• •	•	• •					•					• •				•	•						•		• •		• •			• •		
				•											• •													• •					• •		
				•											• •													• •					• •		
•	•		• •	•						•					• •				•	•						•		• •		•			• •		
	•		• •	•											• •				•	•						•		• •		• •					
	•		• •	•											• •				•	•						•		• •		• •					
•	•		• •	•						•					• •				•	•						•		• •		• •					
	•		• •	•											• •				•	•						•		• •		• •					
			• •	•											• •				•	•						•		• •		• •					
															• •																				
															• •																		. ,		

It's not known it		•
PÇPSPACE!	PSPACE	•
All of these complexity	A/QMA	•
Classes ore separated by		•
problem F such that	BQPMA	•
$P^{F} \neq NP^{F}$ .	BPPNP	•
(There also exists an t		•
where. Pt=NPF.)		•
where $\Gamma = NP'$	P	•

IP=PSPACE	.       .
but separated 6-	9 randours oracle!
$C_{i} \neq \frac{2}{2}$	$\forall f \neq$
1       1	.       .

Why is BQPSPACE?
Gisti ve can sutfichetly approximate
$\langle z U w \rangle = t \sigma \sigma \eta$
Z, we zoilg and width N cipcuit U.
< z (U/w) > =
$\sum_{x_{11}x_{21}-1}^{1} \langle z   G_1(x_1) \langle x_1   G_2)   x_2 \rangle \cdots \langle x_{21}   G_{\ell}(x_{2}) \rangle$
$V = G_1 G_2 = G_2$

$M_{-1}$ , $\mathcal{S} \mid C_{-}$	··· + ···· -) ···· -)/ ····	
<u>Jeleting vil</u> some g	Value algor. The s	
· · · · · · · · · · · · · · · · · · ·		
1. Simon's problem		
I. Reducing tactoring to	period - Finding	
TT. Place activation of	) Decia) - Findia	
	or percoo interry in a	
	· · • · · · · · · · · · · · · ·	

I. Simon's problem
First, recall Deutsch's problem can be solved in O(1) on
quantum computer.
Input: - black box Function
F: {0113 ~>> {0113
which is promised to be either: i) Constant, or ii) belanced, meaning #F-1(0) = #F-1(1). Problem: Decide Mether F is constant or belanced.
Classically, requires 2 <sup>n-1</sup> +1 evaluations of F. "Oracle separation" of BRP and P.

Since BP We separ	> is "realistic" classical computing, can ate RPP and BRP?
Warning! 1 Know	PEBPPEBQPEPSPACE, and we don't IF P=PSPACE!
ls three	an ORACLE separation of BPP and BQP?

Simon's problem replace of X	c. <del>f</del> .
Given black box/oracle Function of X1= 2m	
F: {0,13" -> {0,13t (k2n-1)	· · · · · · · · · · ·
which is promised to saturity	· · · · · · · · · · ·
$f(x) = f(y)$ if and only if $x - y \in \{0, s\}$ For some of $\{0, 1\}^n$	· · · · · · · · · · · · ·
Problem: Find S.	· · · · · · · · · · ·
Can't be solved in BPPF. Even a probabilistic	· · · · · · · · · · ·
algorithm requires at least 2 yurris to oracle	· · · · · · · · · · ·
to Find $x \neq y$ with $f(x) = f(y)$ .	· · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · ·
Sinon's algorithm Suppose have usual "quatum oracle" For F  $U_{\Gamma}: (\mathbb{C}^{\lambda})^{\otimes m} \otimes (\mathbb{C}^{\lambda})^{\otimes k} \longrightarrow (\mathbb{C}^{\lambda})^{\otimes n} \otimes (\mathbb{C}^{\lambda})^{\otimes k}$  $|x,y\rangle \rightarrow |x,y \oplus F(x))$ Use simple circuit 10><sup>8</sup>"-[H<sup>®</sup>"-[-] Hont  $|F(x)\rangle$ 

0)" [10" Shorthind	Fr
107-[H]- [07-[H]-	

Output is (H@n @1d) 0 UF 0 (H@n@1d) 10h) @10k> J V2 (1-1)  $= (H^{\otimes n} \otimes J_{d}) \circ U_{F} \left( \frac{1}{2^{h/2}} \sum_{x=0}^{2^{h-1}} |x\rangle / 0^{h} \right)$  $= H^{\otimes n} \otimes IJ\left(\frac{1}{2^{n/2}} \sum_{x} |x\rangle| + (x)\right)$  $=\frac{1}{\lambda^{n}}\int_{-1}^{\infty}(-1)^{x} \langle 1 | \gamma \rangle F(x) \rangle$  $\times$  1 $\gamma$ dot product over Z/2Z  $H^{\otimes n} \sum_{x} |x\rangle = \frac{1}{\lambda^{n/2}} \sum_{x,y} (-1)^{x,y} |y\rangle$ 

$=\frac{1}{2\pi}\sum_{X,X}(-1)^{X,X} Y\rangle E(X)\rangle$
If we measure the y output in computational basis, then
probability of seens a specific bit string y E 20,15 is
$ \left\  \frac{1}{2} \sum_{x} (-1) \left( \frac{1}{2} \left( \frac{x}{x} \right) \right) \right\  $
$\frac{1}{2^{n}} \sum_{x} (-1)^{x \cdot y}  F(x) ^{2} = \frac{1}{2^{n}} \sum_{z \in I} [(-1)^{x_{z} \cdot y} + (-1)^{(x_{z} + S) \cdot y}]  z ^{2}$
where $f^{-1}(z) = \{x_{2}, x_{2} + s\}$

$\left\ \frac{1}{1^{n}}\sum_{x_{2}}\left[\left(-1\right)^{x_{2}}+\left(-1\right)^{(x_{2}+s)}-y\right]\right\ _{2}\right\ _{1}^{2}=\int_{1}^{\infty}O  if  y=s=1 \mod d$
2 E I 1 1 F Y-S=0 mod 2
destruction intertirment 1/1 and s70
Take away:
Get uniform distribution on Constructur interforence
$\{0,s\}^{\perp} = \{x \in \{0 \}^{n} \mid x \cdot s = 0 \mod a\}$
Performing experiment & times, get X1, X21, X2 such
that Xi · S = O mod 2 for all S. Generate { 01 s 32
with probability $\geq 1 - \frac{150, s^2}{2} = 1 - \frac{1}{2}$
$\mathcal{L}^{\ell}$ $\mathcal{L}^{\ell-n+1}$

[F x1,, Xl	generate, Can recover 5 as
(Mon - trivial)	So UTion at to a second a se
	· · · · · · · · · · · · · · · · · · ·
	/X·C=O mod 2
	$X, \zeta = D$ mod d
	· · · · · · · · · · · · · · · · · · ·
	X. S=O mod

What	fhe	heck	just	4 appens o	, ?
· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · ·			
Mat exactly	Cecre	st it are	ml: zex · · · ·		

Hidden Subgroup problem Input: Finitely generated group G, set X and black b. x function  $F: G \rightarrow X$ that is constant on cosets of HEG (and distinct on distinct cosets). Problem: Find generators of H.

Abelian hidden s well understood	<b>subgrou</b> ( So)ua	$\frac{1}{2}$ $p^{\prime}c$	blems RQP	<b>?</b> )	
	Mary	impor	tast	Spec:~	J
Cases among th	em, "	cluding			
- Deutsch's problem - Simon's problem	2 Contri	1ed	·         ·		.     .     .     .     .     .     .       .     .     .     .     .     .     .       .     .     .     .     .     .     .       .     .     .     .     .     .     .       .     .     .     .     .     .     .       .     .     .     .     .     .     .       .     .     .     .     .     .     .
- discrete log - order - Finding	Vseful		.         .         .         .         .           .         .         .         .         .         .           .         .         .         .         .         .         .           .         .         .         .         .         .         .         .           .         .         .         .         .         .         .         .           .         .         .         .         .         .         .         .           .         .         .         .         .         .         .         .		.         .
- period - Finding	· · · · · · · · · ·	· · · · · · · · ·	· · · · · · ·	· · · · · · · · ·	· · · · · · · · ·

Basic idea:	con implene	t Four:	r tronsf	brang on	
· · · · · · · · · · · · · · · · · · ·	abelian gro	ups on	quartum	computer	
· · · · · · · · · · · · · · ·			· · · · · · · · · ·		
Routher flra	n to this a	errally,	it's cut	to the ch	~ <del>}~</del>
	<b>7</b>				
	· · · · · · · · · · · · · · · · · · ·				
	actorin	d · · · · · ·	· · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · ·
· · · · · · · · · · <b>/</b> · · · · · · · · · · · · · · · · · ·			· · · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · ·

II. Reducing Factoring to period Finding
Factoring Problem
Given integer N in binary, compute prime factorization $N = p_1^{k_1} \cdots p_k^{k_k}$
reduces to
Given N>1, Find 14 KCN that divides N, or, iF not possible, return "Is Prime."
Note: Miller-Rabin (BPP) or Agrawal-Kayal-Saxena (P) primality test allow us to assume N composite.

Factor-Finding For composite integers reduces in BPP to	
Order - Finding Given N and ILXLN with gcd (x,N)=1, Find Smallest F71 such that	· · · · · · · · · · · · · · · · · · ·
$x^{r} = 1 \mod N$	
Soir is order of $x$ in $(\mathbb{Z}/N\mathbb{Z})^X$ .	· · · ·
	· · · ·
	· · · ·

Factor - Funding - Order - Finding
Two basic steps
1. X2=1 mod N but X = + 1 mod N yields
Factor (either gcd (x-1,N) or gcd (x+1,N))
2. A calonly chosen y E(2/NZ) has even order r
and y 1/2 # # 1 mod N w/ large probability.
IF we have such as you they
$gcd(\gamma^{r/2} \pm 1, N)$ will
be a factor, by step 1.

Factor - Fin	Jing g	Order - Fi	nd ing in	BPP	
(vo precise	2 theorems				
1. Suppose	N Kas	L bets, is c	ourposite, and	2 × 4	atistic,
<b></b>		- · · · · · · · · · · · · · ·	· · · · · · · · · ·		
	$(1 \leftarrow \times \leftarrow \Lambda$	/::::::::::			
	1,2-1				
	$\sum X^{-1} = -1$	mod /V			
	TX ==+	mod	· · · · · · · · · · · · · · · · · · ·		
<u> </u>					
The eith	v- gcd (	$x - 1, \mathcal{N}$ ) or	gcd ( X + 1,	N) is	9
No-trivial	Factor	$F = \Lambda I$			
		· · · · · · · · · · · · · · · · · · ·			· · · · · · · · · · ·

2. Suppose N odd, composite, and N=p, KI is prime Factorization- IF 14× EN-1 is a Uniformity candom integer w/ gcd(x,N)=1 and r is order of x in  $(2/N2)^{\times}$ , then Prob (reven and x 1/2 = - 1 mod N) 2 1 - 1 - 21.  $\frac{2}{2}$ 

1. IF N even, return 2. (O(1))
$\lambda = a^{b}, a^{2}, b^{2}, ceturn a.$ (O(L <sup>2</sup> ))
3. Choose condour 1 L X L N-1.  F gcd(X,N)>1, (O(L2))
return ged.
4. Find r, the order at x in (ZINZ) X. (Usi quartum Computer)
S. If rowd, pick another X. (O(1))
6. If r even, trut if god (x 1/2+1, N) or god (x 1/2-1, N)
is a factor. IF neither is, the pick another X.
(have Factor-Finding + RPD order-Finding

•	i (					f	₹	S F	?}	ר כי ני	Ċ	JL	Ś	G	?Ρ	) ) )		.f		 	, , ,	د م	• •	С	<u>م</u> م	• •	ى	40		· · ·	•	• •	•	•	• •	•	•	•	• •	•	•	• •
•	· ·	•	•	•	· ·	•	Ċ		9			1 15		F	- 1 c	שר שר	; ~	) 9	. (	E	f	ß	6	λĮ	2	· ·	•	· ·	•	••••	•	· ·	•	•	· ·	•	•	•	· ·	•	•	· ·
•	· ·		l.	2-	י י ר	•		F	90		ь Но	, F	; ; /	ا م ر	· · ·	E	ſ			Q	Ą		•	}	50	· · · ·	•	· ·	•	· ·	•	· ·	•	•	· ·	•	•	•	· ·	•	•	· ·
•	• •	•	•	•	• •	•	•	•	• •		•	•	•	•	••••	•	•	•	• •	• •	•	•	• •	• •	•	• •	•	• •	•	• •	•	• •	•	•	• •	•	•	•	• •	•	•	• •
•	· ·	•	•	•	· ·	•	•	•	· ·		•	•	•	•	• •	•	•	•	• •	• •	•	•	•	• •	•	· ·	•	• •	•	••••	•	• •	•	•	· ·	•	•	•	· ·	•	•	· ·
•	· ·	•	•	•	· ·	•	•	•	· ·		•	•	•	•	· ·	•	•	•		· ·	•	•	• •	• •	•	· ·	•	· ·	•	· ·	•	· ·	•	•	· ·	•	•	•	· ·	•	•	· ·
•	• •	•		•	• •	•	•		· ·		•	•	•	•	••••		•	•		· ·	•		• •	• •	•	• •	•	• •	•	• •	•	• •		•	• •	•			• •	•		• •
•	· ·	•	•	•	• •	•	•	•	· ·		•	•	•	•	· ·	•	•	•	• •	• •	•	•	• •	• •	•	• •	•	· ·	•	••••	•	• •	•	•	· ·	•	•	•	· ·	•	•	· ·
•	· ·	•	•	•	· ·	•	•	•	· ·		•	•	•	•	· ·	•	•	•	• •	• •	•	•	•	· ·	•	· ·	•	· ·	•	· ·	•	· ·	•	•	· ·	•	•	•	· ·	•	•	· ·
	• •																																									

III. Phase estimation and order-finding
Physe estimation is 9 general procedure
for estimating eigenvalues of a unitary (or Harmitian)
operator U when we have controlled - Un operator
accessible as oracles for every jr.
Unitary V + evector (4) ~ > & where U/4) = ettil (2)
Controlled - U 7 .
$(-\upsilon i:  j\rangle \otimes  z_i\rangle \rightarrow  j\rangle \otimes (\upsilon i u\rangle.$

Quantum phase estimation protocol (sons protocol)
Input: (i) Black box For C-Ur
(ii) eigenvector /u) with U/u) = e u/u/u)
(Tii) integer n
(iv) $\xi > 0$ (e.g. $\xi = \frac{1}{3}$ )
Output: u-bit approximation l'u to lu
Performance:= O(t2) contine, where t= n+ Moy (2+ 2)]
- $O_{ne}$ call to $C - U^{\gamma}$ $C = O_{n}$
- Succeeds ~/ probability at lest 1-E.
· · · · · · · · · · · · · · · · · · ·

I won't discuss circuits For phase estimation may but instead how to reduce order finding to it.
Wont to Find order of X in (Z/NZ)X.
Use
(): In For XX mod NY : FOENEN-1
$\langle 1_{\gamma} \rangle$ ; $F N \leq \gamma \leq 2^{L}$
where Lis # bits in description of N.
· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·

Eigenvectors of U: (not all of them...)  $(u_s) = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-\partial \pi i sk}{r}\right) | x^k \mod N$ For 04545-1. Eignvalues: e 277.15/ssues: C-U8? Mobiler exponentiation ... [us]? Propose 15 [us] = [00--01] instead ...

• •	0	د	· · · · ·		•	• •					•	•			•	• •		-			1					· ·	, T				•	0		j.				• •	 •	•
	•			1	•		6			ッ	•	÷ S		5	•		C	<u> </u>	0		l :	1	Ue	20			7	9	$\sim$	13	21	•		4	50	- 1	(	~	 •	•
				•																																				
• •	٠					• •			•				• •	٠					•	• •			• •			• •		• •								• •		• •		
																			•																					
			• •			• •																				• •		• •					• •					• •		
• •			• •			• •							•			• •				• •			• •		•	• •		• •					• •			• •		• •	 •	
						• •																				• •		• •												
• •			• •			• •							• •			• •				• •			• •		•	• •		• •					• •			• •		• •		•
		•		•	•	• •	•				•						•				•	•				• •		• •				•		•						
			• •			• •																				• •		• •					• •							
• •			• •			• •							• •			• •				• •			• •			• •		• •					• •			• •		• •		
								•										•							•															
																																						a 7		
• •			• •			• •							• •			• •										• •		• •					• •			• •		• •		
• •			• •			• •							•			• •				• •			• •		•	• •		• •					• •			• •		• •		
			• •			• •																				• •		• •										• •		
• •			• •			• •						•	• •			• •			•				• •			• •		• •		•						• •		• •		

	,		 	
Meeting G. Z: Quan	tum error	rorrection	 	
L. Werview			 	
T Direction f			 	
	ectors		 	

I. Over view
Should "fully programmable" quatures computers actually be built,
it is generally expected that BRP will be correct abstraction
of quantum polynomial time.
But realistically, two practical issues to grapple with when
engineering a quantum computer:
le Storing quantum states in a stable way.
L. Implementing Correct quantum gartes.
What's the proslem: NOISC.
1. Word un States very delicate. 1 ricidentally measuring Charges the states) 2. Unitary group U(n) is not discrete ("Continuous errors" can compound.)

In theory, these issues should be solvable, by two to chniques:
1. Runtum error correcting codes
2. Fault tolerant quantum computation.
We will Focus on the first, but let me First address the second.
Basic idea of fault-tolerance:
in addition to using codes to store states, use encoded gualing
gates.
$ 0\rangle - H$ $ 0\rangle^{\otimes 7} + FT \text{ prepare} FT \text{ prepare} FT H \text{ correct} FT H \text{ correct} FT FT \text{ prepare} FT \text{ prepare} FT H \text{ correct} FT H$
$ 0\rangle$ $ 0\rangle^{\otimes 7} + FT \text{ prepare}_{ 0_L\rangle} FT \text{ error}_{correct} FT \text{ error}_{correct} FT \text{ error}_{correct}$
· · · · · · · · · · · · · · · · · · ·

Concatenating two codes (encoding one code inside another) costs polynomial overhead, but can lead to an exponential improvement in error rate. Iterating yields:

Threshold theorem for quantum computation: A quantum circuit containing p(n) gates may be simulated with probability of error at most  $\epsilon$  using

 $O(\operatorname{poly}(\log p(n)/\epsilon)p(n)) \tag{10.116}$ 

gates on hardware whose components fail with probability at most p, provided p is below some constant *threshold*,  $p < p_{th}$ , and given reasonable assumptions about the noise in the underlying hardware.

p~ 10-6

Note:	fault tolerant classical computing much easier to
· · · · · · · ·	achieve. It thinks a constant error rate OLELY3
· · · · · · · ·	at every stip of a classical Boolean circuit
· · · · · · · ·	causing independent but Flip errors, then
· · · · · · · ·	repetition Codes, e.g.
· · · · · · · ·	0 H7 000 Majority rule
	AND > AND AND AND AND
· · · · · · · · ·	allow us to make x Y x, Y1 x2 Y2 x3 Y3
· · · · · · · · ·	270 as small as we'd like.
Quartur	m analog of this code is not very good

What's a quantum code?	•
An n-qubit quantum error-correcting code of dimension d is	•
a Hilbert subspace	
$\mathcal{H} \subseteq \mathcal{C}^{\lambda} \otimes \mathcal{C}^{\lambda} \otimes \cdots \otimes \mathcal{C}^{\lambda} = (\mathcal{C}^{\lambda})^{\otimes n} \cong \mathcal{C}^{\lambda^{n}}$	•
n "physical" quarts (n called "length" & code)	•
IF 1- 1K II a H and the kind out the	
1) d-d, then we say i cheades in logical forms.	
It is sometimes called the Code space.	•
It is sometimes called the code space. Not all subspaces are some! How they sit in ([2) <sup>8</sup> M	•
It is sometimes called the code space. Not all subspaces are some! How they sit in ([2) <sup>84</sup> wir.t. tensor decomposition matters	
It of a then we say it chooses it is great forth. It is sometimes called the code space. Not all subspaces are some! How they sit in ([2) <sup>804</sup> wir.t. tensor decomposition matters	

Con	pare las	;de (	(C 2) @	25				· · · ·	· · · · ·			· · · ·	•
   	À	f <sub>1</sub> = Span	٥٥٥ کے	··•07,  1	/1 17	, ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;	("(cp	puntun etit:	)	e")		· · · ·	•
· · · · · ·	74	2 = span	[ 000	0>,	100-	07	3 (*	frivia	L Ca	le")		· · · ·	•
Both	2-dimen	sional, s.	+1.e-1	both	encode	2 9	Sin	gle	quh	;}		· · ·	•
 	· · · · · · · · ·	H			H,	· · · · ·	· · ·	· · ·	· · · · ·	· · ·		· · ·	0
5+	Hi apper	rs <sup>r</sup> Sp	rend o	-t m	nore.	· · · ·	· · ·	· · ·	· · · · ·	· · ·	· · ·	••••	•
How	to make	pre cise?	· · · · · ·	· · · · · ·		· · · · ·	· · · ·	· · ·	· · · · ·	· · ·		· · ·	•
· · · · · ·	· · · · · · · · · ·		· · · · · ·	· · · · · ·	· · · ·	· · · ·	· · ·	· · ·	· · · · ·	· · ·	• •	· · ·	•
· · · · · ·	· · · · · · · · · ·		· · · · · ·						· · · ·			· · ·	

Local bit Flip error supported on single qubit
Not true for 1000> and 1111>.
More importantly, It, is an entire subspoke, not just the
two basis states. Since quantum computers wat to exploit superposition and entackment, we want to detect and
Correct errors on <u>orbitrary states</u> in the codespace.
The repetition code will be able to detect
up to n-1 bit flip errors and correct up to [1/2]

Recoll  $\frac{1}{2} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Given  $(b_1, b_2, \dots, b_n) \in (\mathbb{C}^2)^{\otimes n}$ , define  $X_{j}|b_{j}b_{j}\cdots b_{n}\rangle = |\partial_{(\mathbb{C}^{2})^{\otimes j-1}} \otimes X \otimes |\partial_{(\mathbb{C}^{2})^{\otimes n-j}}|b_{j}b_{j}\cdots b_{n}\rangle$ =  $|b_1 - b_1 \rangle \otimes X |b_1 \rangle \otimes |b_{1+1} - b_h \rangle$ So Xi is a bit Flip error at it qubit We define Zi similaly, as a (relater) planse flip at the ith gubit.

E.g. n= S. 74 = spon { [000007, [1111]}}
$X_{1}X_{4}\left(\sqrt{\frac{3}{5}} 00000\rangle+\sqrt{\frac{3}{5}} 1111\rangle\right)$
三月10010>+月01101>
"Majority rule" corrects His X, Xy error CORRECTLY.
$X_{2}X_{3}X_{5}(\sqrt{\frac{2}{5}} 00000) + \sqrt{\frac{2}{5}} 11111)$ = $\sqrt{\frac{2}{5}} 01101) + \sqrt{\frac{2}{5}} 10010\rangle$
We could measure to see that errors occurred, but
will recover incorrect state.

('ve been uncaretu). How do ve s	see ensis occured
withat spailing the states?	
Do measurement ~/ operators	
Po = 100000/600001 + /11111/ 11111</td <td>(mo error) provined</td>	(mo error) provined
$P_{1} = (10000) \times (10000) + (01111) \times (01111)$	(bit flip on 1) prosumed
$P_{2} =  0 000 \times (01000  +  10 11) \times (1011)$	(Lit Flip on 2) presumed
: P <sub>k</sub> = /11000×11000/+ /00111><00111)	(Lit Flips on 1+2) presured
Р = /101007<10100)+ /01011><01011)	(bit flips on 1+3) presured)
$P_{N} = (00011) < 00011 + (11100) < (11100)$ $I - P_{1} - P_{2} - \dots - P_{N}$	(bit Flips on 4+5) presumed

So repetition code good at detecting bit Flip en	°~S
However, H, is still a bad QUANTUM code. A single local 2 error on H, Can swap orthogonal states:	
$\frac{2}{\sqrt{2}} \left( \frac{ 0007 +  1117 }{\sqrt{2}} \right) = \frac{ 0007 -  1117 }{\sqrt{2}}$	
H, can not detect any Z errors.	
	· · · · · · · · · · ·

So we're Two key	left issues	high	and (	dry 5	now.
l. Do go exist?	od quai	tun erro	( Co((	ecting	Codes
2. What X or	about 2?	ercors	Hbort	aren 17	<ul> <li>· · · · · · · · · · · · · · · · · · ·</li></ul>
	· · · · · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · ·

I. <u>C</u>	);ccre-	$t:_{t}$ at :	r f	eryos	• <u> </u>	• • •	· · · · ·	· · · ·	· · · ·	· · · ·	· · · · ·	· · · · · ·		
Fa	- trat	tely,	( <b>†</b>	two	era		97C	Corre	e ctable	ء ٢		any	· · · · · ·	
	) p 9 (	con	nbin	ation	of	thear	), <u>,</u> , , , , , , , , , , , , , , , , ,	· · · ·	· · · ·		· · · · ·	· · · · ·		
$\mathcal{N}$	leed		make	Sone	+4;	~gs	prec	ise	Forst:		· · · · ·	· · · · · ·		
· · ·	. Er	for	a)	noise.	· · · · ·	· · ·	· • · · ·	· · · ·	· · · ·	· · · · ·	· · · · ·	· · · · · ·	· · · · · · ·	
j j	- De	tectak	le	ecror	a	Code	J ist	and a	· · · ·	· · · · ·	· · · · ·	· · · · · ·	· · · · · · ·	
3	S. Co	rrecta	ble	error	· · · ·	· · ·	· · · · ·	· · · · ·	· · · ·		· · · · ·	· · · · · ·	· · · · · · ·	
· · ·	· · ·	· · · · · ·	· · · · ·		· · · ·	· · ·	· · · · ·	· · · · ·	· · · · ·	· · · · ·	· · · · ·	· · · · · ·	· · · · · · ·	
							· · · ·	· · · · ·						
• • •	· · ·					• • •	• • • •			• • • •	• • • •			
• • •	· · ·		· · · · ·	· · · · ·	· · · ·		· · · · ·	· · · ·	· · · ·	· · · ·	· · · · ·	· · · · · ·	· · · · · ·	
If ) $f \in (\mathbb{C}^2)^{\otimes n}$ , a noise (or error) space is any subspace $\mathcal{E} \subseteq \mathcal{B}((\mathbb{C}^2)^{\otimes n}) = all linear tractions atoms(=Mat((\mathbb{C}^2)^{\otimes n}))$														
---														
An error is my EEE.														
We say if detects $E$ ; $F$ exists $\lambda_E C$ such that $\langle \Psi   E   \Psi \rangle = \lambda_E \langle \Psi   \Psi \rangle$ For all $ \Psi \rangle,  \Psi \rangle \in \mathcal{A}$ . $IF P$ is otherword prejection onto it. Equivalent to $I \cdot \Psi = 1$														
Enviring $PE(14) = \lambda_E(14)$ operators $f_{-}$ decide whether $For all (14) \in \mathcal{H}$ . after $E$ acts, IF answer is "tos" (hopens $\gamma_{-}$ prob. $(\lambda_E 2)$ , we still have $14$ ?														

The distance of H is smallest dEN such that
there exists an error supported on d qubits that
)It can not detect.
(Trivial and repetition codes both have distance 1.)
H corrects errors from E if for all X, YEE
It detects Xty.
Theorem This is correct definition of "correcting errors
From E." Ley it's equivalent to requiring there
exist a "error correcting procedure."
· · · · · · · · · · · · · · · · · · ·

		• •	· · +	11
Eq	υί	/ 9	en l	M

Theorem 10.1: (Quantum error-correction conditions) Let C be a quantum code, and let P be the projector onto C. Suppose  $\mathcal{E}$  is a quantum operation with operation elements  $\{E_i\}$ . A necessary and sufficient condition for the existence of an error-correction operation  $\mathcal{R}$  correcting  $\mathcal{E}$  on C is that

 $PE_i^{\dagger}E_jP = \alpha_{ij}P,$ 

(10.16)

for some Hermitian matrix  $\alpha$  of complex numbers.

Take - aways
1. IF H corrects/detects X and Y, then it
corrects/detects aX+by.
2. dist It > 2k if and only if It corrects all
errars on k qubits.
3. Because products of X's and Z's and I's
generate B((C2)BK), suffices to correct
them on all k-gulit subsets in order
to correct ALL k-qubit errors.
Theorem At corrects all errors on the gubits it
and only if it detects all errors that are products
of at most 2K Xi's and Zi's.

•	A	1e	e T	  ;~	.) 0,	•	٩,	<i> </i> :	P T	· ·	T		i i	· ·	С. а	, de		•	• •	0	•	• •	0	•	•	• •	•	• •	0	• •	•	•	• •	•		• •	•	• •	•	•	•
	 			· · ·	ר י		رار	•	- ↓		•	•		ا م	•	• •	•	•	• •	•	•	• •	•	•		•••	•	• •	•	• •	•	•	• •	•	•	• •	•	• •	•	•	•
•	۲. ۲	• •	ľ	77	0	€ V	· >	•			ر بر ب	•		ve		• •	•	•	• •	•	•	• •			•	• •	•	• •	•	• •	•	•	••••	•	•	• •	0	• •	•		•
	• •		•	• •			• •	0		• •	•	0	• •	0		• •	•		• •	0		• •	0		0	• •	•	• •	0	• •			• •			• •	0	• •			
•	• •			• •			• •			• •		0	• •			• •		•	• •	0		• •		•		• •		• •		• •			• •	•		• •	0	• •		•	•
		•	•					•	•		•	•		•			•						•	•			•		•		•			•	•		•		•	•	•
•		•	•		•	•		•	•		•	•		•			•			•	•		•	•					•		•		• •	•	•		•	• •	•	•	•
	 	•	•	• •	•	•		•	•	 	•	•		•	•		•	•		•	•	• •	•	•	•	• •		• •	•		•	•	••••	•	•	• •	•	• •		•	•
•	• •	•	•	• •	•	•	• •	•	•	• •	•	•	• •	•	•	• •	•		• •	•	•	• •	•		•	• •	•	•••	•	• •	•	•	•••	•	•	•••	•	• •	•		•
				• •		•	• •	•				•				• •	•			•		• •			•			• •	•				• •		•			• •			•
	· ·	•	•	• •	•		••••	•	•	· ·	•	•	• •	•	•	• •	•	•	• •	•	•	• •	•	•	•	• •	•	· ·	•		•	•	• •	•		• •	•	• •		•	•
		•	•		•	•		•	•		•	•		•	•		•	•		•	•	• •		•					•		•	•			•		•	• •	•	•	•
	• •	•	•	• •	•	•	• •	•	•	• •	•	•		•			•			•	•	• •	•	•	•		•		•		•		• •	•	•	• •	•	• •	•	•	•
•	• •	•	•	• •	•	•	• •	•	•	• •	•	•	• •	•	•	• •	•	•	• •	•	•	• •	•	•		•••	•	• •	•	• •	•	•	• •	•	•	• •	•	• •	•	•	•
•	• •	•	•	• •	•	•	• •	•	•	• •	•	•	• •	•	•	• •	•		• •	•	•	• •	•			•••	•	• •	•	• •	•		• •	•	•	• •	•	• •	•		•
	• •				•	•	• •	•	•	• •		•	• •	•	•	• •		•	• •			• •		•		• •	•	• •	•	• •			• •	•	•	• •	•	• •	•	•	•

Historical note:
Toric code was introduced by Kitaer AFTER
the stybiliser Formalism was developed, by Calderbart,
Gotteman, Knill, Roms, Shor, Sterne, et al
Toric code is nice b/c it generalizes in differed
i) Statiliur codes, Z/L chain complexes, systolic geometry, ii) other "anyonic models" (i.e. topological quatum Field theory) and topological quatum computations (hardware - based approach to Fault tolerance, not just error correction)

In q nutshell: Stabilizer formalism is a way to convert							
classical linear codes our {0,13" = 17 (or other finite fields)							
into quatum codes. Codespace is a common eigespace of "stabilizers", which are tusor products of X's or Z's.							
More precisely: isotropic set space of IF du c/							
symplectic form correspond to statilizer codes,							
· · · · · · · · · · · · · · · · · · ·							

I. Toric	Code					· · · · ·	· · · · · · · · · · · ·
lapet:	NXN	grid	On	a foru	<b>&gt;</b>		
	· · · · · · · ·	· · · · · · ·	7 <u></u> .	· · · · · ·			
	· · · · · · · ·	· · · · · · ·	•••••	· · · · · · ·			
	· · · · · · · · · · ·	· · · · · · ·		<u> </u>			
	· · · · · · · · ·			· · · ·			
		· · · · · · · ·					
				· · · ·			
	· · · · · · · · · · ·						
				· · · · · · ·			
	<b></b>	<b>_</b>	<u>&gt;</u>	<b>_</b>			
	o vetu	· · · · · · ·					
Output:	A 7 (ou	e H	vith				
	- 1.	ר וו	2		1.1	• • • • •	
	leng	in d	N N		- d'Etance		
	- dim	ension	4 (+1	~ 10485a	gubits)		

Construction l. Put a gubit ()  $P_{u}$ on each edge (2n1)  $V_{ij} = V_{ij}$ 2. For each vertex V, define: X = X V X Vs X VE X (order dorsa lt matter) For each 2-cell P ("plaquette"): Zp=ZpvZpsZpeZp (order dusselt matter) 3. Codespore is H = { 14 ) ∈ (C2) 02" X 14 ) = 2p 14 ) = 14 ) ∀P, v 3 So, It is common + l eigenspice of all vertex and plaquette operator

 $\phi V_N$ XV/ bNb, bE bw> = (X16N) @ (X/6S) @ (X16E)  $\otimes (X/ \downarrow )$ = IGN GS GE EN  $\chi = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$  $7 = \left( \begin{array}{c} 1 \\ 0 \end{array} \right)$ 

$\underline{Claim}: Jim H = 4.$
Proof: Note all approtors commute: (:-stitled on
$[X_{v_1}, X_{v_2}] = [Z_{P_1}, Z_{P_2}] = [X_{v_1}, Z_{P_2}] = 0.$ Nover prove
So they can be simultaneously diagonalized. Note eigeworkey
of XV and Ep are ± 1. Thus dim H 20.
Also note two relations
$\prod_{v} X_{v} = \int_{\mathcal{O}} \int_{\mathbb{C}^{2}} \mathbb{P}^{2v^{2}} = \prod_{p} \mathbb{C}_{p}.$
In Fact, there are no more. (Generalities on stabilities
(oder would let us stop there.)
· · · · · · · · · · · · · · · · · · ·

Why is  $[X_{v_1}, z_p] = 0$ ? IF XV and Zp have disjont supports, obviously they commute P<sub>3</sub> (erg.  $(\chi_{\otimes 1})(1 \otimes Z) |_{A \to Y}$ = (X&Z) (95) = (1 & Z) (X & 1) / 9 b)

I and P overlap) X, Zp Suppose )= X, X, X, X, X, 232723 934  $\frac{q_{5}}{=252_{6}X_{3}X_{4}Z_{3}Z_{4}X_{1}X_{2}}$ 71 = 2526×323×424×1×1 V 72 7 = (-1) (-1) ZS Zb ZzXZZYXYX  $= \frac{1}{2} P \chi_{V}$  $\chi_{v} = \chi_{1}\chi_{s}\chi_{2}\chi_{4}$  $Z_p = Z_3 Z_4 Z_5 Z_1$ |XZ=-5X|  $X = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ 

Know It is some Hilbert space, and
$\dim_{\mathcal{C}} \mathcal{H} = k$ if and only if $\dim_{\mathcal{C}} \mathcal{B}(\mathcal{H}) \cong k^{2}$
So let's compute B(H), General non-sense:
$\mathcal{B}(\mathcal{H}) \cong \mathcal{B}/\mathcal{I}$
where $\mathcal{Z} = \{A \in \mathcal{B}(\mathbb{C}^2)^{\otimes_{2n^2}}\} \mid [A, X_{\mathcal{J}}] = O = [A, Z_{\mathcal{P}}] \}$
I = Ideal generated by Xv-1 and Zp-1.
Mexipoint: Xu-lof (20) & and Has topologically meaning ful generators!

If c is a loop in I-skeletan,	
de Fine	
در: 11 Ze ودد	
IF d a loop in dual l-skeleton, d	<mark>⋧<mark>ੵ</mark><mark>ੵੵੵੵੵੵੵੵੵੑ ● ੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੑੵੑ ● ੑੑੑੑ</mark></mark>
det:~e	
$X_{j} =    X_{e}$ eed	
Note Z <sub>C1</sub> XJ E Z For all c1d.	$(W_{4}?)$
Even better:	· · · · · · · · · · · · · · · · · · ·
& is generated by Zc a	~J XJ.

Note, it c bounds dick D (more generally, is 2/2 homologically trivial) the Zc = TT Zp. PED IF & bounds disk D then  $(X_{ij} = T_{ij} X_{ij} = T_{ij}$ VED In particular, if and d bound, then Ec and XJ act by identity on H, i.e. tc=1 mod The End XJ=1 mod Th.  $\bigtriangledown$ 

. . . . . . . . . . **. .** . . . . . 🖌 . . . .

Corollary (F c=c'	$H_{1}(S' \times S', Z)$	?122), then
Zc/7	$= Z_{c}/H$ .	(Upper bands,
(+ J=d' 1- H, (S'x)	51, 2122), the	dim 23(7+) = 11
XJ  H	= XJ.172.	· · · · · · · · · · · · · · · · · · ·
Converse also ti	rue. To prove	this, Suffices to
Check that		Conclusion:
C11 /11C2 102		$\dim \mathcal{B}(H) = 16$
yield 16 linearly		
independent operators		Jim )7 = 4
$\sim$ $\mathcal{H}$		

What J	o Codeve	ctors "r	eally i lool	k like?	(2= spen {  07,117}
Suppose	14) E À	t. The	2p/7>	= 147	t = ( +1)
C <sup>2</sup>	· · · · · · · · · · · · · · · · · · ·		6-6 )=7	2,7,2	16.66-6
C <sup>2</sup> P	• C <sup>2</sup>			, b, + b, + b, + b,	
				-()	10, b, bE b,
		· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	• • • • • • • • • •	
So, Zp	[4] = [	4) For	all p me	ns 127 ,	nust be in
So, Zp spar of	[4] = [ 5754'5 5	4) For totes whe	all p me	ns 147 . bots econd	ench Pis even.
So, Zp spar of	[4) = [ 5754'5 5	4) For totes whe	all p me	ns 147 . bots econd	ench P is even.
Son Zp span of	[4) = [ 575'5 S	¥) F=r tates whe	oll p me	ns 147 . bots erand	ench P is even.
Sol Zp spar of	[4) = [ 5754'5 5	¥) F=r totes whe	all p me	ns 147 bits econd	ench P is even.
Son Zp span of	[4) = 1 575'5 S	¥) F=r tates whe	or    P me	ns 147 r bots econd	ench Pis even.

· · · · · · · · · · · · · · · · · · ·		16,656 <u>5</u> 6 <b>w</b>	)= 15 <sub>N</sub>	δ <sub>s</sub> δ <sub>E</sub>	کر ک	· · · · ·	<ul> <li>.</li> <li>.&lt;</li></ul>	· · · · ·	•
Suppose Where	1777 hrs 6~+65+1	Some Mon Zo >E + Son = 0	ro amplitu mod For c	inch pla	ong 16, ng vette	ь, Ь Р)	2n2		
Since A -mplitude	v (24) = (24 e along	7, then 1 Av 16, 62.	74) m. b 2 2. ).	ist Uni	او ج		<ul> <li></li></ul>		
.         .	.       .	.	.         .         .         .         .         .         .           .         .         .         .         .         .         .         .           .         .         .         .         .         .         .         .           .         .         .         .         .         .         .         .           .         .         .         .         .         .         .         .           .         .         .         .         .         .         .         .           .         .         .         .         .         .         .         .         .           .         .         .         .         .         .         .         .         .	.     .     .     .     .       .     .     .     .     .       .     .     .     .     .       .     .     .     .     .       .     .     .     .     .       .     .     .     .     .       .     .     .     .     .       .     .     .     .     .		.         .         .           .         .         .           .         .         .           .         .         .           .         .         .           .         .         .           .         .         .           .         .         .           .         .         .           .         .         .	<ul> <li>.</li> <li>.&lt;</li></ul>	· · · · · ·	· · ·

Note: Au preserves	C1 d1	· · · ·		· · ·	· · · ·	
Ste mod 2 and Sispasty	· · · · · · · · ·					· · · · ·
eec, She mod d. Sof	· · · · · · · · ·			· · ·	· · ·	
$eec_{j}$ $H_{1}(S'xS', 2/2)$	2			· · ·	· · · ·	· · · · ·
Can check: it						رۍ ۹۳
eec, $eec$ , $eec$ ,	· · · · · ·	· · ·	· · · · ·	· · ·		· · · · ·
Sibe = Sibe mod d, then I eec,			V <u>}</u> 1 1	Such	, -10	
$A_{v_1}A_{v_2} - A_{v_2}   b_1 - b_{2u^2} =   b_1' - b_{2u^2}$	1 \ 24 <sup>2</sup>	).	· · · · ·	· · ·	· · ·	· · · · ·
Note: need plaquette condition to preve it!	· · · · · ·	· · · ·	· · · · ·			· · · · ·

Conclusion there's a basis of codevectors in bijection with elements of H, (S'XS', Z/22). More procisely, that is basic where each element is an equal superposition of all cellular representatives of give class in Z/L homo bogy Eng. (000-0) is NOT in A-But it represts 9 2/2 Cellular CId Cycle (nomely the O cycle). (an build a code vector by sammy 0 . . . . . . . . . . . . over collular rep's in some homology Class, 100--07 + ---



							_	• •										• •			• •				• •								
		$\mathbf{i}$		6			6)	• •		- C				• •							• •		• •		• •				• •			• •	
		$\mathcal{I}$	Ś	<b>`</b> . O	<b>1</b> 0	e	1	• •		Ú	$\mathcal{O}$	'₽ι	)0	عل	2										• •				• •				
							- 1					I. (																					
	• •																				• •												
•								• •						• •						•	• •				• •				• •				
								• •													• •												
•											•			• •		•				•	• •												
•											•			• •		•				•	• •												
								•													• •		• •		• •				• •				
								• •															• •						• •				
																							• •										
•	• •			•				• •						• •			•	• •		•	• •		• •		• •				• •			• •	
																	•			•			•		•								
•	• •			•		•		• •						• •			•			•	• •		•		• •				• •		•	• •	
								• •									•						• •		• •				• •			• •	
	• •							• •						• •							• •		•		• •				•			• •	
								• •									•						• •		• •				• •		•	• •	
									-																								

Meeting 9	1.2: Toric code	II, and	Statailizer	Formalism
I. Toric	Code code vectors	and	distance	
I. Stabil	lizer formalism	· · · · · · · ·	· · · · · · · · · ·	
	· · · · · · · · · · · · · · ·			
· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · ·	
· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·

Construction REMINDER	
l. Put a qubit ()	
on each edge (2n1)	$\mathbf{e}_{\mathbf{e}} = \mathbf{e}_{\mathbf{e}} + $
2. For each vertex V, define:	
X = X V X Vs X VE X (order doesn't Matter)	
For each 2-cell P ("plaquette"):	
Zp=Zp, Zp, Zp, Zp, Zp, (order desalt montfer)	
3. Codespore is	· · · · · · · · · · · · · · · · · · ·
$H = \{   \Psi \rangle \in (\mathbb{C}^2)^{\otimes 2^n}   X_v   \Psi \rangle =$	2p14>=14> 4P, v3
So, It is common the eigenspace of al	Il vertex and plaquette operation

I. Toric Code Codevectors and distance
Finish claim from last fime:
There's a basis of H "in natural" bijection with
H, (S'XS'; Z/2). The brois elements are equal
superpositions of all cellular cycle representatives
in given homology class.
Prost: Identify computational basis vector
$ b_1b_2\cdots b_{2n+1}\rangle \in (\mathbb{C}^2)^{\otimes 2n+2}$
with a Z/2 cellular 1-chain. That is, (b, b, b)
encodes a toram 2/2 linear combination of edges
in cellulation of S'xS'.

Thus, could say  $(\mathbb{C}^2)^{\otimes dm^2} = \operatorname{Span}_{\mathbb{C}} (C_1^{\operatorname{cell}}(S' \times S'; \mathbb{Z}/2\mathbb{Z})).$ Note 16.62 -- 62.27 represents a cycle if F bp + bp + bp + bp = 0 mod 2 iff  $Z_p(b_1b_2\cdots b_{2L_2}) = [b_1b_2\cdots b_{2L_3})$ For all plaquettes/2-cells P. So if 14> EH, ve see 147 is a superposition of cellular 1-cycles.

From last time, give 14) EH with (bib	2 <sup>.</sup> - 621.2	+)=c	7
the condition XVIY)= 147 Forces	· · · · · ·	· · · · · · · ·	
$\langle 6, 6_2 \cdots 6_{2n^2} \rangle \chi_{v_1} \chi_{v_2} \cdots \chi_{v_q} \rangle = c.$	· · · · · ·	· · · · · · · · ·	· · · · · ·
Moreover cycles (bibj bing and (bibj b	6262	Sut:sty	
$X_{v_1} X_{v_2} - X_{v_2}   L_1 L_2 - L_{2L^2} =   L_1' L_2' - L_{2L^2} >$	· · · · · ·		· · · · · ·
For some X's ; F and only iF	· · · · · ·	· · · · · · · ·	· · · · · ·
S. b' = S. bo mod and			
		· · · · · · · · ·	
Sibe = Sibe mod d		· · · · · · · ·	
where c, and c, as in hime			دځ . ۹ <sup>۳</sup>

Distance?
Recally a code can detect all k-qubit errors
if and only if it can detect all products
of X; and Z; supported on at most k qubits.
Spose
$E = X_{i_{1}}^{\alpha'} X_{i_{1}}^{\alpha'} \cdots X_{i_{k}}^{\alpha'} \neq_{i_{1}}^{\beta_{1}} \neq_{i_{1}}^{\beta_{2}} \cdots \neq_{i_{k}}^{\beta_{k}} \qquad (\alpha_{j_{1}}, \beta_{j_{1}} = O_{1})$
is such an error.
IF E is a product of Xi's and Zp's, the E
acts trivially on it, here is not as error. IFE
takes it outside itself, then we can detect that
because one of the Xv's or Zp's will be violated.

Main issue: iF E preserves it setwise but not
pointwises That is, if Elift is nontrivial. In this
Case, we know From last time that E/H must
he a product of loop or dual loop operators:
lf c is a loop in l-skeletan, define
$z_c = \Pi z_c$
(F d a loop in dui) l'skeleta,
det:~e
$X_{j} =    \wedge e$ eed

			c l S		\$، 2°	م ملا *	p S		pr t	o o R	]~  }	(9) (9)	).	<b>G</b>	) N S		· • • • •	7			+		γc	,/e	, <del> </del>		ria fL						С И Ч	<b>0</b>	l ta	0 ; V	a   ion	7		;	<b>1 1 1 1 1 1 1 1 1 1</b>	• • • • • • •				
	-		Ji	ict	دىر	, , , ,	, () () ()	; ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;	) =	~~~~	h	1 1	۲	s Z		t s		p	(c	)	]	•	С С	É	2	се 1	" (	۲ ۲		۲S	- - - -	22 <sub>1</sub>	(ጉ) የ	)     	E E		} 1	£ (	56	e i	H,	2	•	•	· · ·	•
											Ŷ	م` د					•																													
• •			• •															• •						•	• •				•				•				•								• •	
	•							• •			•	•	•											•	• •				•	• •						•										
																																													• •	
		•	• •			•						•			•	•	•	• •						•	• •								•					-							• •	
	•																						•				•					•													• •	

Toric code con be generalized to: -kts homology of any cell compley - any Z/2 chain complex.

II. Stabilizer formalism (after Callerback - Rains - Shor - Sloone)
Toric code is an example of a statoilive code.
Given qubits, define <u>error group</u>
$E = E_{n} \leq (/(2^{n}) = (/(\mathbb{C}^{2})^{\otimes n})$
to consist of all tease avaluate of team
$\pm \omega_1 \otimes \omega_2 \otimes \cdots \otimes \omega_n$ or $\pm i \omega_1 \otimes \omega_2 \otimes \cdots \otimes \omega_n$
where $w_{i} = [d, X, ], \text{ or } t$
Recall > (0 - i)
$ \left( \begin{array}{c} 1 \\ -1 \end{array} \right) = \left( \begin{array}{c} 1 \end{array} \right) = \left( \begin{array}{c} 1 \\ -1 \end{array} \right) = \left( \begin{array}{c} 1 \end{array}$
Figure 1-9(20)

Know if we co on $k$ gubits, $t$ $U(2^{n})$ supporte	an detect all error then we can dete id on gt mat	rs from E ect all errors K qubits.	Sported From
(More precise)y, the end occur with	stabilizer formaliser Some protectivity.	n presumes However, mith	X, Y, Z nat too
much overland,	implies ability to	o correct erro	ors in
other models)		· · · · · · · · · · · · · · ·	· · · · · · · · · · · · ·
			· · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · ·	· · · · · · · · · · · · ·

Classical warm-up
Classical Z/2 linear code is subspace C= (Z/2)?
(2/2) is of cause space of all possible states,
but it is also space at all possible errors.
Error REC iff e is undetertable. (C. is - abspace)
( corrects set of errors SIFF For all
$S, t \in \mathcal{I}, e, T \ll \mathcal{I} \subseteq \mathcal{I} \subseteq \mathcal{I}$
sites, either site disjoint from S
s, $t \in S$ , $e, t \neq C$ . or $s+t \notin C$ . disjoint from S.
s, t $\in$ s, $e$ , two s+t $\notin$ C. or s+t $\notin$ C.
sites, either site of disjoint from S. or site C. disjoint from S.
In quantum setting, a nontrivial
----------------------------------
on codespice (e.g. Xv in
So, we look for two
$\zeta \leq \zeta'$
Anley of A
203, the the
F-r this to work, need S' to
want 5 abelign. How
(Compare fore code!)

$Order(E) = \lambda^{2++\lambda}$
$C_{entor}(\Xi) = C(E) = \{ \pm I, \pm i I \}$
$\overline{E} := E/C(E) \cong (\mathbb{Z}/\lambda)^{2n}$
IF eEE, can uniquely write
$e = i^{\lambda} X(a) Z(b)$
where $\lambda \in \mathbb{Z}/4$ and Litwise addition
$X(a) c\rangle =  a+c\rangle$ (bit fip eners where $q_{ij} \neq 0$ )
2(L) (c) = (-1) / (c) (phone errors where
a,b,c e (Z/2) dot product mod 2

$lF = i^{\lambda} X(a) \frac{1}{2}(b),  e' = i^{\lambda'} X(a') \frac{1}{2}(b'),  then$
$ee' = i^{\lambda + \lambda'} \chi(a) Z(b) \chi(a') Z(b')$
$= \frac{1}{2}^{\lambda+\lambda'} (-1)^{\gamma' \cdot \mathbf{b}} X (-1) X (-1) \frac{1}{2} (\mathbf{b}) \frac{1}{2} (\mathbf{b}) \frac{1}{2} (\mathbf{b})$
$= \frac{1}{2} \lambda + \lambda' (-1)^{2' \cdot b} \chi(a') \chi(a) \chi(a) \frac{1}{2} (b') \frac{1}{2} (b)$
$= i^{\lambda + \lambda'} (-1)^{\alpha' \cdot b} (-1)^{\alpha \cdot b'} \chi (\alpha') \frac{1}{2} (b') \chi (\alpha) \frac{1}{2} (b)$
$= (-1)^{a,b'+=',b} ee'.$
So e and e' commute if and only if
$a \cdot b' + a' \cdot b = 0  (in  \mathbb{Z}/2)  (X) = \mathbb{Z}$
Write $\vec{e} = (a b)  \vec{e} (a' b')$ for images in $\vec{E} \cdot \vec{e}$
e mo t commute iff e as e original in E wit (i)

ē,ē' orthogonal for all ē,ē' E Š < Ē.
In other words, Sabelian if and only if Sis totally isotropic.
E.g. $\{\chi(a)\} = \mathcal{E}[\chi]$ or $\{\xi(b)\} = \mathcal{E}[\lambda]$ .
Beware! (*) is a symplectic inner product on (2/2)2n
$ F(a b) \cdot (a' b') = a \cdot b' + a' \cdot b, then$
$(a b) \cdot (a b) = \lambda a \cdot b = D.$

Centralizer of S is exactly the preimage of
$\overline{S}^{\perp}$ (Note: $\overline{S} \leq \overline{S}^{\perp}$ if $\overline{S}$
is isotropic!)
Let codesport le
$24 = \{ 1+ \}   e   2+ \} =   2+ \} \text{ for ell } e \in S \}.$
Define the symplectic weight of (a/b)E(2/2)24
is # of nonzero pairs (airbi) when we write
(916) = (91,,91   L(,,bn)

	Tl	<u>r</u>				, ,	· ·	(	F	•	•	0	/;,		2	י ג/		 	Ŝ	•	-L	h	-	h	•		is	•	۲	٢	łra	»pi	د	• •	مرا	7	-	S	70	~`¥	ple		tic	•	•	• •
	Fo		مە	j	•	-	-1	کو(	h'	•	r J	4		i	י בי			7		C	)	ĸ	•	0	l'îc	n	15		ہ م	,)		۰ ۲	J	د ج	•	من	+	Ļ	•		•	•	•••	•	•	• •
• •	д	; د'ر	<u>+</u>	27	C	•		•	•	•	•	•	•	•	•	•				•	•	•	•	•	•	•		•	•	•	• •	•	•		•	•	•	• •	•	•	•	•	• •	•	•	• •
••••	•	•	•	•	•	•				C	J	Ċ,		n	ı jir	•	1	V	4	х х	دما	, 1		)	5	-	• •	•	•	•	• •	•	•	•	•		•	••••	•	•	0	•	• •	0	•	• •
• •		•	•	•	•	•				•	•	•	V	E	S		- -		Ŝ		•	•	•	•	•	•	• •	•	•	•		•	•	• •	•	•	•	• •	•	•	•	•	· ·	•	•	• •
• •	•	•	•	•		•		•		•	•	•	•	•	•					•	•	•	•	•	•	•	• •	•	•	•	• •	•	•		•	•		• •	•	•	•	•	• •	0		• •
• •	•	•	0	0	•	•				0		0	•		•	•		• •		0	•	0	•	•	•		• •	0	•	•	• •	•	0	•	•	•	•	• •	0	•	0		• •	0	•	• •
• •	•	•	•	•	•	•			•	•	•	•	•	•	•	•	•	• •		•	•	•	•	•	•	•	• •	•	•		• •	•	•	• •	•	•	•	• •	•	•	•	•	••••	•	•	• •
• •	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•				•	•	•	•	•	•	•	• •	•	•	•	• •	•	•	•	•	•	•	• •	•	•	•	•	• •	•	•	• •
• •	•	•	0	0	•	•			•	0	•	0	•	•	•	•	•	• •		0	•	0	•	•	•	•	• •	0	•	•	• •		•	•	•	•	•	• •	0	•	•	•	•••	0	•	• •
• •		•	•		•	•						•	•			•					•	•	•				• •		•	•	• •	•	•		•			• •		•	•		• •	•		• •
• •		•	•	•	•	•				•	•	•	•	•	•	•				•	•	•	•	•	•	•	• •	•	•	•	• •	•	•		•	•		• •	•	•	•		• •	•		• •
• •	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	• •		•	•	•	•	•	•	•	• •	•	•	•	• •	•	•	• •	•	•	•	• •	•	•	•	•	••••	•	•	• •
• •	•	•	•	•	•	•		•	•	0	•	•	•	•	•	•				0	•	•	•	•	•			•	•	•		•	•	•	•	•	•	• •	•	•	•	•	• •	0	•	• •

Meeting 10.1: From TQFT to TQC, q Brief history	•
I. Atiyah + Witten	
I. Reshetikhin - Turgev + Turgev	•
II. Turgev - Viro + Barrett-Westbury	•
IV. Kitaer + Freedman	•
I. Freedman - Kitaev - Larsen - Wang	•
II. Levin-Wen	•
	•
· · · · · · · · · · · · · · · · · · ·	•
· · · · · · · · · · · · · · · · · · ·	•
	•
	•

Kitanis interesting tor interesting toric code
(and generalizations to other finite groups I will
mention later) was to address tault tolorance
problem USING HARDWARE.
He doesn't use laguage of TQFT directly, but
was clearly inspired by it, since anyous were
understood to be the "particles" that can arise
in certain exotic (topological) QFTS.
· · · · · · · · · · · · · · · · · · ·
······································

I. Atiyoh + Witten	· · · · · · · · · · · · · · · · · · ·
1988 - Atiyah defines	TOPOLOGICAL QUANTUM FIELD THEORIES by Michael ATIYAH
topological quartum Field theory. Mathematically rigorous! Uses language of	To Red Thom on his 65th birthday. <b>1. Introduction</b> In recent years there has been a remarkable renaissance in the relation between Geometry and Physics. This relation involves the most advanced and sophisticated ideas on each side and appears to be extremely deep. The traditional links between the two subjects, as embodied for example in Einstein's Theory of General Relativity or in Maxwell's Equations for Electro-Magnetism are concerned essentially with classical fields of force, governed by differential equations, and their geometrical interpretation. The new feature of present developments is that links are being established between <i>quantum</i> physics and <i>topology</i> . It is no longer the purely <i>local</i> aspects that are involved but their global counterparts. In a very general sense this should not be too surprising. Both quantum theory and topology are characterized by discrete phenomena emerging from a continuous background. However, the realization that this vague philosophical view-point could be translated into reasonably precise and significant mathematical statements is mainly due to the efforts of Edward Witten who, in a variety of directions, has shown the insight that can be derived by examining the topological aspects of quantum
cobordisms and Functors. Inspired by work (esp.	The best starting point is undoubtedly Witten's paper [11] where he explained the geometric meaning of super-symmetry. It is well-known that the quantum Hamil- tonian corresponding to a classical particle moving on a Riemannian manifold is just P.J.B. IHES (1988)
of Witten) on (general, not-entirely-rigorous) supersymmet	ric grating
Field theory, and Segel's axia	ms for conformal field theory

<u>TQFT in a nutshell</u>
K: a Field (or other unital commutative sing)
Cob(J): d-dimensional oriented cobordism category
Objects (Cob(d)): oriented, smooth, closed d-manifolds
Mor ((ob (d)): oriented, smooth (d+1)-manifolds M,
w/ dM= Zol Zi. M is a morphisms
$\mathcal{M}: \mathcal{L}_{0}  \mathcal{L}_{1}$
Q: disjoint union
A (d+1)-dimensional TQFT is a "Orrespecting linearization
of (ob(d), i.e. q & functor Z: (ob(d) > Vec(1k)
might "> vell assume Finite d'un.

Schematric d=21 lk=C (a a) 21 (-) Z(Z) the F.d. vector spine over C  $M^{3}$  $| \neg Z(M): Z(\Sigma_{o}) \neg Z(\Sigma_{i})$ J DL. linear map

Hermitian and Unitary TQFT
If k= a, we can ask jadjoint
$\sum (M) - \sum (M) + K$
M w/ ceversed orientation and suppord
Low Jose nieres
For all M. IF this holds, call the TQFT hormeter
For all M. IF this holds, call the TQFT hormites It is unitary if moreover, the pairing
For all M. IF this holds, call the TQFT hormites It is usitary if moreover, the pairing
For all M. IF this holds, call the TQFT horists It is unitary iF moreover, the pairing \$

50000 5,×1- $2(\Sigma \times I): 2(\Sigma) \otimes 2(-\Sigma) \longrightarrow 2(\phi) = \mathbb{C}$ 2(5)× deg) Vector grad IF this priving is positive definite and 2 is Hermitian, then we say Z is unitary. If Z is unitary, the Z(S) is a Hilbert space

E.g. (Toric Code) 2(2):= Span H, (S; Z/2) if I connacted  $2(\Sigma_{1} \sqcup \Sigma_{2}) = 2(\Sigma_{1}) \otimes 2(\Sigma_{2})$ IF JM = Lou Di, then  $2(M): 2(\Sigma_{n}) \rightarrow 2(\Sigma_{n})$ linearizes the correspondence  $M^* \in H_1(\mathcal{L}_0; \mathbb{Z}/2) \times H_1(\mathcal{L}_1; \mathbb{Z}/2)$  $M^* = \left\{ (\alpha, \beta) \mid [\alpha] = \mathcal{L}\beta \right\} \text{ in } H_1(M; \mathbb{Z}/2) \right\}$ 

Also in 1988,	Atiyah asked		· · · · · · · · · · · · · · ·	· · · · ·
ls there	an intrinsically	3 - dimensilon	a) explanation	· · · · ·
For why -	Jones polynomia	, l is an i	nvor:at F	· · · · ·
Knots?	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · ·		· · · · ·
	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		
Jones had di	Krowered it i	~ 1954 Und	erctood only	
Jones had di diagrammatical	iccovered it i. In at that the	1 1964. Und Ime, ergs	erstood only a normalization	F
Jones had di diagrammatical Kauffman bri	iccovered it i. Ily at that fi acket	7 1984. Und (me, ergs	erstood only a normalization	£
Jones had di diagrammatical Kauffman bri $\langle 0 \rangle = -q^{1}$	is covered it is $  _{y} = t$ that the final f	7 1984. Und ime, e.gs	erstood only a mormalization	£
Jones had di diagrammatical Kauffman bri $\langle 0 \rangle = -q^{1}$	iccovered it i. $  _{\gamma} = t$ that the final fi	η 1984. Und ime, e.g. −s	erstood only s normalization	£
Jones had di diagrammatical Kauffman bri $\langle 0 \rangle = -q^{2}$ $\langle \times \rangle = -q$	iccovered it is $N_{y} = t$ that the first is acket $N_{z} = q^{-1/2}$ $N_{4}(z)(z) = q^{2}$	η 1984. Und ime, erg. as	erstood only s normalization	£

1989 - Witten argues (not 100% rigorously) that for of a cost of unity, the KowfFman bracket Communications in Cay be Used to build Commun. Math. Phys. 121, 351-399 (1989) Mathematical Physics © Springer-Verlag 1989 g (2+1)-Jim TQFT. Based on quantizing Chern-Simons theory w/ Quantum Field Theory and the Jones Polynomial \* gauge group G= SU(2), Edward Witten \*\* School of Natural Sciences, Institute for Advanced Study, Olden Lane, Princeton, Different roots of unity NJ 08540, USA yield different TQFTS. **Abstract.** It is shown that 2 + 1 dimensional quantum Yang-Mills theory, with an action consisting purely of the Chern-Simons term, is exactly soluble and gives a natural framework for understanding the Jones polynomial of knot theory in three dimensional terms. In this version, the Jones polynomial can be generalized from  $S^3$  to arbitrary three manifolds, giving invariants of three manifolds that are computable from a surgery presentation. These results shed a surprising new light on conformal field theory in 1 + 1 dimensions.

I. Reshetikhin-Turnev + Turnev
Witten's construction not rigorous. Eventually made
(igerous, but in the meantime Reschetikhin and Turow
did give a mathematically rigorous construction
Using quasi-triangular Hopf algebras and
diagrammatic (or <u>skein</u> ) constructions of TQFTs.
The Witten-Resherikhin-Turaev uses the category
of finite dimensional representations of a guari-triangular
Hopt algebra. When one uses Ug sly, one recover
the Joney-Kauffman TQFT for that specific q.

Turner generalized Further to arbitrary
Modular Tensor Categories.
(IF H is q.tr. Hopt algebra, the Rep (H) is q modular tusir category.)
It turns at, once - extended (2+1) - dimisional /QFTS are entirely determined by a modular fersor
Category (w/ one addition-1 smill choice) Recertish theorem of Douglas, Schourse-Pries
Vicary, et al

A once - extend TQFT is of "usual (2+1)- dinas: april
TQFT that also associates data to ever (2-1)-mite
in functorial way
Making this precise involves "higher tensor cartegories"
$E_{\mathcal{B}}$
$M^{>} \longrightarrow Z(M): Z(\partial M_{o}) \xrightarrow{\sim} Z(\partial M_{i})$
2 - Vector spre Z(E)
S' 1-> category Z(S1)
it is a module tensor category
· · · · · · · · · · · · · · · · · · ·

One can study	eve	Furth extuded	TQFTs
eg- fully-exte	nded	TQFT	· · · · · · · · · · · · · · · · · ·
	· · · · · · · ·		
d+1 Mon; Fold		(inconst	
d manitold		vector space	
2-1 mon: told		Category	
d-2 Martold		2-category	
	<b>.</b> <b>.</b>	· · · · · · · · · · · · · · · · · · ·	
	· · · · · · · · · ·	$\left(\begin{array}{c} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{array}\right) = \left(\begin{array}{c} \cdot \\ \cdot $	
ct. point		o - category	· · · · · · · · · · · · · · · · · ·
Baez-Dolan colordi	sus Lyp	stheris proved	67 Lurie.

II. Turgev- Viro + Barrett-Westbury
Turner-Viro shared (1993?) you to Construct
a Fully extended 3-d TRFT From a
modular tensor category.
Dor't get anything that Reshe tikhin - Turger Construction
doesn't already provider
Barrett-Westlary defined spherical fusor
Categories, and showed Turapu-Viro Turaks"
For any splaring) (user category

5' 1-> Dritel'é ceter 2(C) (always a modular teator catagory) 5 F> Vector space 2(5) (9greus R-T construction for 2(C))

$E_{g}$ C = G - Vec	
the category of G-graded Finite diman) Direc D.	vector spaces
Object in C looks litze	
$V = \bigoplus_{\alpha \in G} V_{\mathcal{G}}$	· ·
where Vg is a F.J. Vect. spar.	. .

Morphism  $F: V = \bigoplus_{g \in G} V_g \longrightarrow W = \bigoplus_{i_i \in G} W_i$ is a sum of live anaps F3: Vg ~ Wg1  $F = \bigoplus F_g$ geG.

 $V \otimes W = (\bigoplus_{g} V_{g}) \otimes (\bigoplus_{h} W_{h})$  $= \bigoplus (V \otimes W)_{\chi}$  $(V \otimes W)_{X} = \bigoplus_{\substack{g,h\\gh=X}} V_{g} \otimes W_{h}$ 

· · ·	ł	(:- [-	ן 	e~ :  o	, <sup>1</sup> ج ارر	<u>~</u>	P	-6- -	ər H	ا و	· · ·	e:	sp Ti		182	کر بر				<i>م</i> ہ ر	} 			is vo	°c	e +	'se F	- C	J V	). /c	،// د †		~	ž	· · · · · · · · · · · · · · · · · · ·		· · ·	•
· ·	•	1	G	۲۲ ۲		Ĩ	•	9	<b>7</b> 55	>O	)c:	91	te	)	•	4			• •	, , ,	5			Ve	20		•	• •		• •	•	•			· · ·	•	• •	-
• •				· · · · · · · · · · · · · · · · · · ·	•	· · ·	н н Ф(	)e		•	· ·	i S S	· ·	s S S	ρe Γ	<u>?</u> [ ]	: 9	)	· ·		<u></u> 9	e Se t		· ·						Z				•	· ·	•	· ·	•
•••	•	• •		• •		•••	•	• •	•	•	••••	•	• •	•	•	•••	•	•	• •		••••	•	•	• •	• •		•	• •	•	•••	•	•	• •		• •	•	• •	•
• •			•	• •	•	• •	•	• •		•	• •	•	• •	•		· ·	•	•	• •	•	• •	•		• •				• •		• •	•	•	• •	•	• •	•	• •	
• •	•	• •	0	• •		• •		• •			• •	0	• •	0	0	• •	0	•	• •	0	• •	0	•	• •				o o o o	•	• •	•	•	• •		• •		• •	•
•••	•	• •		• •	•	· ·	•			•	• •	•			•		•	•			• •	•	•				•	• •	•		•	•		•		•		•
• •	•			• •	•	• •	•				• •	•			•	• •	•	•	• •		• •	•	•	· ·				• •	•		•	•	· ·	•		•		
• •	•		•	• •	•	• •	•	• •			• •	•	• •	•	•	• •	•	•	••••	•	• •		•	• •				• •	•	• •	•	•	• •	•	• •	•		

Me	eting	10.2	<u>:</u> Topo	bgicg)	quatum	computi	19, I	· · · · · ·
I.	Anyon	s from	elementar.	exatt	inc in	toric code	<u>.</u>	
II.	TQC	and	TQF		yand	In hm	) <u>,</u>	
· · · · ·		· · · · · ·	· · · · · · · ·		· · · · · · · ·			· · · · · ·
· · · · ·	· · · · · ·	· · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · ·
			· · · · · · · ·	· · · · · · · ·				
· · · · ·		· · · · · ·	· · · · · · · ·	· · · · · · · ·	· · · · · · · ·			· · · · · ·
· · · · ·	· · · · · ·	· · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · ·
· · · · ·	· · · · · ·	· · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · ·
			· · · · · · · ·	· · · · · · · ·				
· · · · ·	· · · · · ·	· · · · · ·		· · · · · · · ·		· · · · · · · ·		· · · · · ·
· · · · ·	· · · · · ·	· · · · · ·	· · · · · · · ·		· · · · · · · ·	· · · · · · · ·	· · · · · · · · ·	· · · · · ·

Given a cellulation w/ N edges of a grus g suffer Sg, toric code yields a 49-dimensional code space $\mathcal{H} \in (\mathbb{C}^2)^{\otimes N}$ $\mathcal{H} = \{  \mathcal{H} \rangle \mid X_{V}  \mathcal{H} \rangle =  \mathcal{H} \rangle = Z_{P}  \mathcal{H} \rangle  \forall vertice v, plaquettes P_{S}^{S}$ We can repackage $\mathcal{H}$ as the grand state space of
foric code Yields a $4^9$ -dimensional code space $24 \in (\mathbb{C}^2)^{\otimes N}$ $24 = \{1^{2}\} \times 1^{2} = 1^{2} = 2_{p}(2^{2})  \forall vertice v, plaquette P}$ We can repactioge $24$ as the grand state space of
$\begin{array}{l} \mathcal{H} \leftarrow (\mathbb{C}^{2}) \otimes \mathcal{N} \\ \mathcal{H} = \left\{ \left[ \mathcal{W} \right\} \right] \times (\mathcal{W}) = \left[ \mathcal{H} \right\} = \mathcal{E}_{p} \left[ \mathcal{W} \right]  \forall vortice \ v, \ plaquette \ P \\ \mathcal{V} = \left\{ a  ve \ package \ \mathcal{H}  as \ dhe \ \tilde{g} \ round \ state \ space \ of \end{array}$
)4 = { 14)   X, 14) = 14) = Zp(4) Vuertier v, plaquettes p} We can repackage it as the ground state space of
We can repactione it as the ground state space of
$H = \sum_{v} (I - X_v) + \sum_{p} (I - 2_p)$
ire. $\mathcal{H} = \ker \mathcal{H}$ . Hermition operator

$X = \begin{pmatrix} \sigma & l \\ 1 & \sigma \end{pmatrix}$	$\int z = \begin{pmatrix} 1 & o \\ o & -1 \end{pmatrix}$
Spac X= { -1, 1}	$sper z = \{-1, 1\}$
$\boxed{\begin{array}{c} 1 \\ -1 \end{array}} = \left( \begin{array}{c} 1 \\ -1 \end{array} \right)$	$ \left( \begin{array}{c} I - 2 = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \right) $
Spec I - X = {0,2}	<pre>Spei I-2 = {0,2}</pre>
Spec $I - X_{r} = \{0, 2\}$	$\int s p = c \ I - 2 p = \{0, 2\}$
Xv's and Zp's	Commute, hence sa do
$I - X_{v}$	$I - 2_p$ 's

Physics intuition: If consists of "Vacuum" or " States with Hamiltonian H.	Zero-energy"
Eigenvectors of H corresponding to NON-zero spec H: OCA, CA, L CA The eigenspace is the state	eign volues?
Sprie For (pairs of) Telementary of this system	porticles"
In Fact, spec H: OL4L8L What is EX, the eigenspace corresponding to	γ <sup>1</sup> .5

More intrition: suppose X, (4) + 14%.
We might say that 127 has a charge or particle
at vertex v. (hontero)
Similarly, if Zp/47 +147, might say 147 has
a (nonzero) Flux through P, or 12) his a "vortex"
on plaquette P.
A lovest energy state i.e. It > EE, must violate
as few of the constraints XVI4>=147, Zp /4>=147
95 possible.
B/c TT X = [d = TT Zp, 14) either violates exactly P two X's or two Zp's.

Recall:
If c is a loop in I-skelitan,
define
$z_{c}$ ; $  $ $z_{e}$ eec
IF d a loop in dual I-skeletan, d
$det: X_{i} = \prod X_{o}$
eed The loop operators generate possible errors of the cook.
A loop operator implements an undetectable and matrixica) error
$H_1(S' \times S'; 2/2)$

•
If c is a parts in I-skeletan,
define 7 - TT 7
It d a path in dual I-skeleta,
$X_j = \prod X_e$ .
(F 14) E H, then Zc 147 and X, 14) are in
E. For inclose, Zc/47 will violate the two Xis

· · · · · · · · · · · · · · · · · · ·	
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·	- <b></b>
<b>♦   ♦   ♦</b>	
	• • • • • • • • • • • • • • • • • • •
	· · · · · · · · · · · · · · · · · · ·
	·
· · · · · · · · · · · · · · · · · · ·	the second secon
	the other had
· · · · · · · · · · · · · · · · · · ·	
a a a a a a a a a a a a a a a a a a a	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·	
	$X, z_{c}(\Psi) = \lambda_{c}(\Psi)$
	$(\mathbf{x}_1, \mathbf{y}_2, \mathbf{y}_1, y$
V = 1 n r = -2 n r	N
$\Lambda_{V_0} \simeq c \left[ \frac{q}{r} \right]^{-2} = c \left[ \frac{q}{r} \right]^{-2}$	$f_{o} = \int \left( \frac{1}{2} \int \frac$
a ang ana aga ana ang ang ang ang ang an	· · · · · · · · · · · · · · · · · · ·
$1 \rightarrow 1 \rightarrow$	· · · · · · · · · · · · · · · · · · ·
and A Mar March 1 and A and a second of C. A share a	and a second product of the second second product of
· · · · · · · · · · · · · · · · · · ·	
	$\sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{i=1}^{n} \sum_{i=1}^{n} \sum_{i=1}^{n} \sum_{i=1}^{n} \sum_{i$
	· · · · · · · · · · · · · · · · · · ·
	· · · · · · · · · · · · · · · · · · ·
	$[1, 1, 2, 2] = \frac{1}{2} \sum_{i=1}^{n} \frac{1}{2} \left[ \frac{1}{2}$
	na na sana ang sina na sana na sana sa sa sa tang tang tang tang sa sana sa sana sa sana sa sana sa sana sa sa Ang

Note: 17 (24) E'24, 2 (14) = 2, 14) if and only if c+c'=0 in  $H_{1}(S'*S'; 2/2)$ Similarly For X2's. a a 🔨 a a Mare generally Or op ours Vice, to other Surface codes

Kitmer's (\$100,000,000?) iden:
Introduce a small number of particles anto
the surface, and move them around in
controlled ways in order to intentionally manipulate
a codestate of the foric code. Because nontrivial
operations occur only ofter doing something "topologically
non trivial," the probability of implementing the
wrong operation can be made small without much
over head.
le other words: "Fault tolerance Fram hardwore"
if you can implement the brix code Hopmiltonian in or lab.
Two related Enformation
---------------------------------------
l. braiding
J. De yn
· · · · · · · · · · · · · · · · · · ·

177) EH Braiding in Kitaeu's unde) ctat w/ state:  $\chi_{j} z_{c} (4)$ 92 4T 95 92 c42 Ex, ( 7, ) 76 P 75  $X_{l} = X_{q_{\delta}} X_{q_{\gamma}} X_{q}$ 7.7 Apply 3 Xl 6 X, Z, (14) 's liter moving Flux or of the changes at of the C stig the second

 $\chi_{\varrho}(\chi_{J}Z_{c}|\psi) = (-1) \chi_{J}Z_{c}|\psi\rangle$ Note: this is true only because of the charge of the ed of the String C. Weird! Moving Flux along a loop acound a charge indenets a nontrivial charge to the state.

The elementary violations of the Stabilizer ( .... the particles) have "han trivial" braiding statistics. Such particles are called enters

Stat ~) (47 EH. "(reate part: clac by  $z_{c_1} z_{c_2}^{-2} - z_{c_2} (\psi) = (\psi)$ This 1- Ins duce 10 XC2X X X X X X porticles and pits us inside Ell x<sup>5</sup>x Loop operators yield a representation of 10 strand brand group!

1-47 EE25 V= Loops: 1-417 4 EZ Representation  $B_{0} \longrightarrow U(V).$ 

(00) H> Z (007 H> Z c, Z (00) "Debn traisting" Start with dim 24 = 4 X/0) @/0) MY GH  $\hat{O}$ Manpulate 10) 82/0> (mr snt another state in 24 by Kecall: (renting pair LOOD Operitor of anyons, act on At like your one around the fashi Xis forus, then annihalate and Z'S

 $24 \approx (28) (2 = 4pers {1007,1017,1107,$  $1112}$ 1000 operates act on 24 by $X \otimes IJ, Z \otimes IJ'$ 6 8 X 100 10 8 2 So, can process quartum into in H by applying loop operators.

Problem	~: +5	br:( (	ode?	 		· ·
W:+4	toric	code,	he	Can	only	· · ·
implen	net	X's	and	2'5		· ·
0- (0	despy	ce V	sig	loop	· · · · · · · · · · ·	· ·
Opera	nt ors,	So	"De"	hs t	must "	· ·
joeg is	うろい	fficier	r fo	gener	te	· ·
guntu	n uni	vesal	opis	01	łf	· · ·

	S: milor	issues	For	braidin	
	· · · · · · · · · · · · · · · · · · ·			J	
· · · · · · · · · · · · · · · · · · ·					
· · · · · · · · · · · · · · · · · · ·					
· · · · · · · · · · · · · · · · · · ·					

Are t Lut	here othe where the	r, Similar Le topologia	setups, cally protected	
opera	rohs are	povertui	Crough to	•
imple	ment a	quartum	vn:versa)	•
gate	set?		·       ·	•
	· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·	•
	· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	•
				•
· · · · · · · · · · ·		· · · · · · · · · · · · · · · · ·		
				•

	.       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .       .         .		
Mont Fr	eedman -	Larsen - l	Verz
.       .		.       .	.       .
.       .			
		· · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
	Mot Fa	Ant Freedman -	Mrt Freedman-Larsen-L

II. TRC a	2 TRFT go hand in hand.
Once-e	xtended (2+1)-dimensional
TQF	s provide a language to
abstra	it away the combinatorial
aspects	of Kitaeu's proposal,
and f	ocus on the topology
of any	ons and their interactions

Me	eting		Topolog	ica) g	vartum con	rputing, I	
I.	Quant	um cil	cuits i	n si le	extended	TQFTs	
II.	Which	TQF	Ts are	BQP.	-Universal?		
	· · · · · · ·		· · · · · · · ·	· · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · ·
							· · · · · · · · · ·
• • • •	· · · · · · ·	· · · · · · · ·	· · · · · · · ·	· · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · ·
· · · ·	· · · · · · ·	· · · · · · · ·	· · · · · · · ·	· · · · · · ·	· · · · · · · · · · ·		· · · · · · · · · · ·
· · · · ·	· · · · · · ·	· · · · · · · · ·	· · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · ·
	· · · · · · ·						· · · · · · · · · ·
· · · ·			· · · · · · · ·	· · · · · · ·	· · · · · · · · · ·	· · · · · · · · · ·	

I. Quantum circuits inside extended TQFTs
Last time: String and loop operators in toric code are
insufficient to build on Universal quantum computer.
However, the idea is useful because string and loop
operators are "topologically protected" operations.
Are there variations of toric code construction
whose topologically protected operations are
power Ful enough to approximate arbitrary quatures
circuits?
· · · · · · · · · · · · · · · · · · ·

Freedman, Larsen, Wang (2007) showed aswer is
$\gamma_{E}$ S.
Specifically, they use the "Jones TOFT with q= e <sup>lxi/s</sup> " This TOFT has other names:
· SU(d) Chern-Simons at level 3 · Witten-Restation-Turger theory for Ugsly, g=e <sup>2πi/s</sup>
expected anyon statistics for fractional quatum Hall effect at certain Filling fraction

We're going to work through the Freedman-Losen-Way
Construction flis week.
First, we need to understand Formal properties of Unitary
once extended (2+1) - dimensional TQFTs (*) This will
allow us to formulate general conditions that allow a
TQFT to be used to simulate quature circuits.
Then, we will need to check the Jones TQFT stisting
these conditions.
· · · · · · · · · · · · · · · · · · ·
(A) I'll say some things later about these restrictions. For now, TQFTs are all Unitary.

RECALL: a (non-extended/ Atiyah style) Unitary (n+1)-dimensional TQFT is a &- Functor From Cob (2+1) to Hilb & O-category & Finite dimensional Hilbert spring (a) surface SH9 Z(S) En Hilbert space  $S_{0} = S_{0}$   $M \rightarrow Z(M): Z(S_{0}) \otimes Z(S_{0}) \rightarrow Z(S_{0})$   $S_{0} = S_{0}$ 

Reasons to like Atigah style (2+1)-dim TRFTs: · Good source of C-valued invariants of closed 3-man Folds  $\left( \begin{array}{c} M \\ M \end{array} \right) \xrightarrow{} 2(m) : 2(\phi) \xrightarrow{} 2(\phi) \\ 11 \\ 11 \\ 11 \end{array} \right)$ Z(M) is a liner map C > C, hunco Z(M) E C.  $\begin{array}{ll} | f M^{3} & is & close \partial_{1} \\ fhen & \partial M = \phi \end{array}$  $\neq Z(M^3) \neq Z(N^3)$ , then M3 & N3,

Reasons to like Atiyah style (I+1)-dim TRFTs: · TRFT axions allow us to compute these invariets via (cut ad poste) e.g. from a Heegaard splitting. IF M= HOLIFI, where Ho and HI are two 2Ho= 2H, gues g had lebodies, me can divide and conqueri  $\frac{1}{2(M)} = \frac{1}{2(H_1)o2(H_0)}$ M= [000]E, (/ H. ///

Get representations of mapping class groups of closed
surfaces from a (2+1) - TQFT. Called quatur
representations of mapping class groups.
IF S is an oriented surface,
MCG(G) := Homeo+ (S)/isotopy
Intuition: MCG(S) is "orientation - preserving homeomorphisms
Modulo isotopy.
MCG(S) = Homeo+ (S) / Gomotopy
$\stackrel{\sim}{=}$ D: FF.o, (S) / isot-py
= Homeon (S)/Normal subgroup of homeomorphilus isotopic to identity

Fig: S-OS are instapic iF fl	↓ ↓ ↓	exist	ά 	· · · · ·	· · ·
H: Sx(o,i) -> S	· · · · ·	· · · · ·	· · · · ·	· · · · ·	· · ·
such flost:	· · · · ·	· · · · ·	· · · ·	· · · · ·	· · ·
(i) $H(x, 0) = F(x)$ $\forall x \in S$	· · · · ·	· · · · ·	· · · · ·	· · · · ·	· · ·
(i) $H(x, l) = q(x)$ $\forall x \in C$	· · · · ·	· · · · ·	· · · · ·	· · · · ·	· · ·
(Fit) H(xit) is a homeomrplism	- ک	<b>~</b>	For	each	· · · ·
(Fit) H(xit) is a homeomrplism Fixed t.			For	erch	· · · ·
(Fit) H(xit) is a homeomy plism Fixed t. (in) H( is continuous.	- ک		For	erch	
(Fit) H(xit) is a homeomrphism Fixed t. (IN) H is continuous.			For	each	

Building quatum reps from TQFT? Given Z, surface Sr and homeomorphism  $F: S \rightarrow S_{1} \quad (a \quad build \quad \mathcal{E}(F): \mathcal{E}(S) \rightarrow \mathcal{E}(S)$ by taking the mapping cylinder of F:  $12(+):=2(M_{+})$ ( ) ) S IF Fig re isotopie, Glue Sx {13 to Susing F MF = Mg, Hus, by EISM MF Sx EoIJ = Kions of TOFT,  $\{s_{2}, c_{1}, c_{2}, c_{3}, c_{4}, c_{1}, c_{2}, c_{1}, c_{1}, c_{2}, c_{2},$ 

Mopping cylinder of F: X -> Y  $M_{\pm} := X \times [oi] \sqcup Y / (x, 1) \sim f(x)$ e.g. X= S', N= Ept3, F constit ango: X 

Gian TQF	T Z: (06/2	$+1) \rightarrow Vec,$
for each su	inface Sr 2	-e set 9 representation
Z: M(6	(S) ~ GL (	2(S)).
· · · · · · · · · · · · · · · · · · ·	Called a	g quatur representia.
Warring: ~/	mare caretal	laxious, might
only get	a projectiu	le representation.
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
5.117 Je		e (epíesetation,

IF TQFT Unitary- (1 will suff:	I is Unitary, then Later, they may only ice :)	the quatum r	epresentations are Uniter-1, but that
5:	McG(S) →	PU(2(	<b>〔</b> \$`)

Can calculate 3-manifold invariate using the quature representations Suppose M is a 3-fold formed by twisting the standard Heegaard splitting of S3 by genus of surface trist three curves using FEMCG(S). Lemmi it Civicg are a complete due system, and [F] EM(G(S) is represented by FI then f(c,),..., f(cg) forms another complete dists system, independent of [epresentine].

T he	(up +	9 9 5-90		in exp	nert)
ζ (	M) - 1	τ ( Π <sub>1</sub> )° ζιτ	-)	70)-	· · · · · · · · · · · · · · ·
This	exprising	2(11) in	trous	6F 71	te.
g va T	an (ep	(esetytun.	· · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · ·
· · · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · ·
· · · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·	 	· · · · · · · · · ·	· · · · · · · · · · · · · ·

		• •		• •				• •		• •		•	• •		• •			• •	• •				• •		• •		• •	
		• •						• •		• •								• •	• •				• •		• •			
																		• •					• •					
																							• •					
																							• •					
																		• •					• •					
																							• •					
																							• •					
																							• •					
																		• •					• •					
										• •								• •					• •					
								•		•					• •			• •					• •				• •	
		• •						• •		• •		•			• •			• •	• •	• •			• •		• •		• •	
		• •		• •				• •		• •			•		• •			• •		• •			• •		• •		• •	
	•	• •		•		• •		• •		• •		•	• •		• •		•	• •	• •	• •		•	• •		• •		• •	
	•	• •		•		• •		• •		• •		•	• •		• •		•	• •	• •	• •		•	• •		• •		• •	
		• •		• •				• •		• •			•		• •			• •		• •			• •		• •		• •	
		• •						• •		• •			• •		• •			• •	• •	• •		•	• •		• •		• •	
	•	• •		•		• •		• •		• •		•	• •		• •		•	• •	• •	• •		•	• •		• •		• •	
		• •						•		•		•			•		•	• •	• •	• •			• •		• •		•	
		• •		• •				•		•		•			• •		•	• •	• •	• •			• •		• •		•	
•		•						•				•			• •				• •				• •		•		• •	
		• •		• •				•		•		•			• •		•	• •	• •	• •			• •		• •		•	
		• •		• •				•		•		•			• •		•	• •	• •	• •			• •		• •		•	
		• •		• •				•		•		•			• •		•	• •	• •	• •			• •		• •		•	
		• •		• •				•		•		•			• •		•	• •	• •	• •			• •		• •		•	
•		•						•				•			• •				• •	• •			• •		•		• •	
		• •		• •		• •		•		• •		•	• •		• •			• •	• •	• •			• •		• •		• •	
		• •		• •		• •		•		• •		•	• •		• •			• •	• •	• •			• •		• •		• •	
		• •						• •		• •			• •		• •			• •	• •	• •		•	• •		• •		• •	
		• •						• •		• •			• •		• •			• •	• •	• •		•	• •		• •		• •	

Rough pass at TQC:
Find a Unitary TQFT whose quatum representation For some surface S is dealed instable
PU(2(S)).
Interpretation: Hilbert space 2(S) is quatum mensery
<ul> <li>Action of a mapping class fEMCG(S) yields</li> <li>q quantum circuit 2 (F): 2(S) -&gt; 2(S).</li> </ul>
to write precise requires choosing guarators of MCG(S),

Theorem (Lickorish-Wallace) MCG(S) is generated by Dehn twists along a specific set it finitely many simple closed curves: ( Charles and Char 9+9-2+9 = 39-2 total generators

Dei bn twist · · · · · Ty: cut N(r), and glue back in with

Suppose  $Z: M(G(S) \rightarrow PU(Z(S)))$  is dense, and let  $F = \prod_{j=1}^{n} T_{j}$ . Applying 2 to F yields  $2(F) = 2(T_{\gamma_1}) \circ 2(T_{\gamma_2}) \circ - \circ 2(T_{\gamma_1}) \circ 2(T_{\gamma_2}) \circ - \circ 2(T_{\gamma_1}) \circ$ AVEUL PICTURE

Using quature representation of MCG(S), we could try to simulate circuite.
However, calt be made correct yet, b/c need
to decompose 2 (S) into tensor products
of subspaces in order to "localize" gub.its
into different regions of surface.
Need extended TQFT!

Me	eting	11.2:	Topolog	yica) g	vatur con	puting, III
I.	Quan	tum c:	revits i	n si de	extended	TQFTs, continued
II.	Which	TQF	Ts are	BRP-	-Universal?	
			· · · · · · · ·			
· · · · ·	· · · · · · ·	· · · · · · · ·	· · · · · · · ·	· · · · · · ·	· · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
				· · · · · · ·	· · · · · · · · · · · ·	
· · · · ·			· · · · · · · ·			
· · · · ·	· · · · · · ·	· · · · · · · ·	· · · · · · · ·	· · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
· · · · ·	· · · · · · ·	· · · · · · · ·		· · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
				· · · · · · ·	· · · · · · · · · · · ·	
			· · · · · · · ·	· · · · · · ·	· · · · · · · · · · · ·	

Last time: can try to use quatum representation of mapping class group of (closed) surface determined by a Unitary TRFT to process quantum information. Problem: don't have any clear my to decompose flibert spre 2(S) its tosor product of subspaces. So, unclear hour to encode quatum circuits... One (unhelpful) ideq: use disconnected surfaces? Quatum representation would generate entaglement....  $2(0 \sigma)g2(0 \sigma)g2(0 \sigma)$ Solution: use extended TRFT!
EXTENDED TOUETS have even nicer cut and paste
properties
In addition to computing Z(M2) by cutting M3 slong
a surface, we can cut surfaces along curves to compute
their state = paces.
To make precise, "extended TQFTs come equipped with
a finite set of $colors$ $C = \{l_1, 2, \dots, r\}$ .
We then define the C-colored, once extended (2+1)-dimensional
Cobordism category C-Cob(2+1).
Contains Cob(2+1) as a subcategory.
Note: what follows is imprecise and incorrect, probably. Why? Don't way
to define extended TRFT or modular tensor category in full detail

C-Cob(2+1) includes new objects: surfaces with (oriented ....) boundary and oriented marked points, with all boundary components and marked points Objects are "C-colored Surfaces 3.7 w/ maked paints " \_\_\_\_\_( \_\_\_\_ \_\_\_) r=10, ie.  $C = \{1, 2, 3, \dots, 10\}$ 

And new morphisme: 3-manifolds with property embedded, C-colored trivalent, oriented ribbon grouphs Nect to allow 3-minut V: Hn "corners.") Technically also need to color trivaled vertices by Note: anothe Morphicus only compose when boundary coloring are compatible

Ribber graph? Ribbon groph Normal grouph U.M.Carter Why? Up to isotopy tel bondary 

```
Celition
```

	As a	F=r & -	Usual Functor	lunextended	ταρτ <sub>ς</sub> ι	an exte	Jed T Unite	°QF⊤ ∽	;
	· · ·	5	: C-	(0b () +1)	> H:	·الح.			
· · · · ·	· · · ·	· · · · ·	· · · · · ·	 	· · · · · · · · · ·	· · · · · · · · ·	  	  	· · · · · · · ·
· · · · ·	· · ·	· · · · ·	· · · · · ·	· · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · ·	  	  	
· · · · ·	· · · ·				· · · · · · · · · ·			· · · · · ·	

In addition to all the axious for Atigah TQFT, an extended TQFT includes axioms that require functoriality w.r.t. culting/pasting of C'colored surfaces. Most important for our purposes:  $2\left(\frac{1}{2}\left(\frac{1}{2}\right)^{3}+\frac{1}{2}\right)$   $=\left(\frac{1}{2}\left(\frac{1}{2}\left(\frac{1}{2}\right)^{3}+\frac{1}{2}\right)\otimes 2\left(\frac{1}{2}\left(\frac{1}{2}\right)^{3}+\frac{1}{2}\right)$   $=\left(\frac{1}{2}\left(\frac{1}{2}\left(\frac{1}{2}\right)^{3}+\frac{1}{2}\right)^{3}+\frac{1}{2}\left(\frac{1}{2}\left(\frac{1}{2}\right)^{3}+\frac{1}{2}\right)$ GLUING AXIOM

Cutting/pasting commute:  $f''' = \int_{1}^{2} \frac{1}{2} \left( \frac{2}{2} - \frac{2}{2} \right) \otimes \frac{1}{2} \left( \frac{2}{2} - \frac{2}{2} \right) \int_{1}^{2} \frac{1}{2} \left( \frac{2}{2} - \frac{2}{2} \right) \frac{1}{2} \left( \frac{2}{2} - \frac{2}{2} \right)$  $\frac{2}{2}\left(\frac{1}{2}\right)^$  $\begin{array}{c} 112 \\ \text{Cut alms} \\ \text{$ along cy

Glving axious allows to specify elements of Z(S) by labelling a complete disk system of S with or I tions and elements of C This yields a vector 2 ( ( 0 0

Note, erg. Z(Din) is Indimesional. The period glue tos yhr. The Jields - Croolored surface homeomorphic to S.

The  $Z(S) \cong Z(S) \otimes Z(DD)$ most la 1-dimensional

Another axiom: the color 1 is special と (enove ) points labelled c-p off bandaries a Se

Gluing axioms allow us to build models of circuits. Hire's one based on closed surfaces. g  $\left\{ \begin{array}{c} a \\ b \\ \vdots \\ b \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \vdots \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \vdots \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \vdots \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \vdots \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \vdots \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \vdots \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \vdots \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \vdots \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \vdots \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \vdots \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\ a \\ \end{array} \right\}$   $\left\{ \begin{array}{c} a \\$ 60 Given 2 and S, ve "Tocalize" quertum rep of MCG(S) along the Sigs.

Vin gluigistate in 2(S) lies in a subspace of the form  $2(S_1, c_1) \otimes 2(S_{21}, c_2) \otimes \cdots \otimes 2(S_{21}, c_1) \otimes 2(T_1, c_{11}, c_{21}, \cdots, c_n)$  $\begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} \quad \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}$ dh 6 102 sphre L/ h disks removed

where  $\mathcal{Z}\left(\mathcal{G}_{i_{1}}c_{i}\right)=\mathcal{Z}\left(\left(i_{2}\right)i_{2}\right)\mathcal{G}$  $2(T_{1}c_{1},c_{n})=2(COO)$ 

Z(S) is s	pound by subspaces of	form
₹(S1, C1) @ ₹	$(S_{2}, c_{r}) \otimes \cdots \otimes \mathcal{E}(S_{n}, c_{n}) \otimes \mathcal{E}$	$E(T, c_{11}c_{21},, c_{4})$
as we var-1	$c_i$ 's in $C = \xi_{i_1} \lambda_{i_2}$ .	,Γ},
· · · · · · · · · · · · · · · · · · ·		
· · · · · · · · · · · · · · · · · · ·		
· · · · · · · · · · · · · · · · · · ·		
· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·		

Setting up circuits Varias ways to do it ---Let's Fix one subspace, i.e. this one. Z(S, c) ⊗ Z(S2, c) Ø ··· ⊗ Z(S, c) ⊗ Z(T, c, c, ···, c) Look at  $\Gamma = \Gamma(c) \leq M(G(S))$ , the subgroup that preserves this subspace.

Dema trists along orange curves generate MCG(S) dy

Another approach: Use braids Consider disk Dn(c) n points all colored by c and boundary colored by 1:  $\begin{pmatrix} + & + & + & + \\ c & c & c & c \end{pmatrix} D_{n}(c)$ Bu acts on Z(Du(c))

Fix K, and consider the Copies of Dk(c) glued together along boundary erg: K=3 <- (c) Ŕ  $B_{L}$   $A D_{L}$  (c).

2 (Dty (c)) Contris of @'s of 2 (DKG (c)) - - $\mathcal{Z}(D_{k}(c)) \otimes \mathcal{Z}(D_{k}(c)) \leq \mathcal{Z}(D_{ky}(c)).$ Con use subgroup of Bres that preserves this subspace to build circuits. What circuite can me simulate?

II. Which TRFTs are BRP-Universal?
(Should assume TQFT is unitary and extended.)
Interasting question in all dimensions.
Has received most attention in dimension 2+1.
$\mathcal{W}_{\mathcal{H}_{\mathcal{H}}}$ ?
· In dimensions 23, too weak
· h dimensions 73, poorly understood. Expected
to be too weak if "fully extended"
· In dimension 3, extended TQFTs all come from
modular tensor contegories via Reshetikhin-Turner
construction. (Combinatorial) - ish

Key guest:	ion give	2, are three colored	· · ·
Surto	reus Supac	quatures representations are	· · · ·
derse	ć~ P	$\mathcal{V}(\mathcal{Z}(S))$ ?	
Forsup.	C'S Nes	you (an simulate / approximit	
			- · · ·
(via Solova	ig - Kitgov a	d additional fricty ) gristing	
(via Solova quatum	ry - Kitgov a circuitk.	d additional tricty) gristing	
(via Solova quatum	c;rcuitc.	d additional tricty) gristing	
(via Solova quatum	ry - Kitgov a circuitk.	2 additional tricty) gristing	

Meeting 12.2	: Topologica)	quantum comp	, ting, IV
I. Universality	From density	of quartury	representations
of Braid	groups		
			· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	
	· · · · · · · · · · · · · · · · ·		
· · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
	· · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · ·	
	· · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · ·	

Fix a C-colored extended unitary TQFT Z and
a color XEC (secretly, X is a simple object
in the unitary modular tensor category determined by 2).
For Convenience:
Assure X is "self dual," meaning 2 treats colored points
$\begin{pmatrix} x & x \\ \cdot & \cdot \\ \cdot $
$\chi$ $\chi$ $\chi$
and also
X and X as identical.
E.g. the "special" color I is self duy). But we will wont
:

DeFine Hilbe	-t space:	CE C		· · · · · · · · · ·	
		to art need	to oright blo	solf Jul	
• • • • • • • • • • • • • • • • • • • •		+			
Z(n; X)	c):= Z	K I			
		X X X	× )		
		n points	on a disl	K	
		· · · · · · · · · · · · · · · ·			
	+ 4 4	ale w/ n			
	colored	paints vill			
		ted Dr.			

Bn acts on Z (ni X,c): C.s. 5-4 "Black board Franing Ē XX χ

Tanjet: 1	plackboard Framing	Convertion		•
Problem:	Drawing ribbons	is anno-y.'ng		
Solution				•
Wacaby:	No Reidemeister	-move	· · · · · · · · · · · · · · · · · · ·	•
		·       ·	·       ·	•

. . . . . . . . . 亡 11 . . . . · · · · · ·/ · · · · · /

Consider D1k =	S2K, 2-sphere	~/ 24 colored points,
and this sphere	x x x x x	$E.g. k = \lambda$
R3		Remark: This frick is
		thy we assume X is self-dual.
Every K-tangle	T in B <sup>3</sup> yield	ds a linear map
; (エ) チ	$\mathbb{G} \longrightarrow \mathcal{E}(S_{1k})$	· · · · · · · · · · · · · · · · · · ·
hence, a vector	T) (namely,	Z(T)(I) in
۶ ( ۵	$(\lambda_k) \cong \mathcal{E}(\lambda_k; X, I)$	

Using this, have	Several Vectors	from "	plonar-	matching
lang les				· · · · · · · · · · · · · · · · · · ·
			シ/	)
			:	
K=}	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · ·	
	J V <			ノレ
				· · · · · · · · · · · · · ·

Fix your Favorite two	crossingless	k-tagles,	دري.
$\begin{array}{c} \mathcal{O} \mathcal{O} \mathcal{O} \cdots \mathcal{O} \\ \mathcal{T} \end{array}$	and (		//s
such that IT and	157 lineer	ly independe	A. Wate
Morally: wat to use	15/3 =  T) and 1	z (24, X s> as comp	1), sutational
Lasis states. 2 issues : orthogonal?	normalized	۶	
	· · · · · · · · · · · · · ·	· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·

0F	Course Hk?	E C2 = spond	{ 10>, 11>}, but chose	<u>د</u>
the	isomorphism	so $ T\rangle$ is	proportional to 10%	<u>ј</u>
	o <b>`</b> }:=	$\frac{ \tau\rangle}{\sqrt{\langle \tau  \tau \rangle}}$	this will come book to have to !	
Let	17 be an	orthonormo	l, erg. Graham - Schm	;.)+
on	(77, 15).			· · · · · ·
H <sub>k</sub>	with these	two basis	vectors will be our	· · · · · ·
que	sit inside of	Z(24; X		· · · · ·

Gates? Well, any dense subset of U(C*@C*) vill be quantum universal.
So: should consider By acting on Z(4K; X, 1),
$\mathbb{C}^{2} \otimes \mathbb{C}^{2} \cong H_{k} \otimes H_{k} \subseteq \mathcal{Z}(\mathcal{L}_{k}; X, I) \otimes \mathcal{Z}(\mathcal{L}_{k}; X, I) \subseteq \mathcal{Z}(\mathcal{L}_{k}; X, I)$

IF quatum representation
$Z: B_{4k} \longrightarrow \bigcup (Z(4k; X_{l}))$
is dense, they in particular every "binary gate" in
U(HK & HL) can be approximately implemented by a
brn; d.
Frest difficulty:
$H_k \otimes H_k$ probably not an invariant subspace of Byf under quatum representation Z: $B_{4k} \longrightarrow U(Z(4k; X_1))$ .
Even worse?
May not be Any broad bE Byk that preserves Hk & Hk and acts nontrivially.

Fortunately: while of practical/engineering importance, in	· · · · · · ·
principle, these issues can be overcome by being cariful	
with Solovay - Kitaev theorems.	
So, we will assume there is a finite subset	· · · · · · ·
BE Bythe that generates a dense subgroup of	· · · · · · ·
	· · · · · · ·
$\cup$ $\cup$ $(\Pi_k, , \Pi_k)$	
· · · · · · · · · · · · · · · · · · ·	· · · · · · ·
· · · · · · · · · · · · · · · · · · ·	· · · · · · ·
	· · · · · · ·
Evaluations & on brails built from Z's acting on Duty nd restricting to Hk & ... & Hk + Z(nk; X1) yields quarters ¢2 Circuit.  $U_{k}$  · · · Ue a la k Ht HK  $C^{2}$   $C^{2}$   $C^{2}$ Julik e &

This shows	we can simulate arbitrary
quantum circ	cuits with X particles in
the IQF	$\frac{1}{2}$
Exam	ples, TQFT,
Jones	by Freedman - Lasen-
$(P^{\circ} Ve^{\circ})$	
E Xam Jours (proved	-Knuffman TQFTs by Freedman - Lasen- Wan

67 K	do topol nots/links	ogical inva 13-maite	~: ~ う しろ
derive this u	d From model o	È relate F computat	75 - 2-

Meeting 13.2 TQC and 3-manifold invariants		
I. "Accept probability of circuit" = "Normalized que	ntum	invariat
II. Approximating quantum invariants w/ qualum comp	outers	
	· · · · ·	· · · · · · ·
· · · · · · · · · · · · · · · · · · ·		
IPAM Summer School (U(LA) on	· · · · ·	
Mathematics of Topological Phases		
6/29 - 9/3		
http://www.ipam.ucla.edu/programs/summer- schools/graduate-summer-school-mathematics-of-	· · · · · ·	
topological-phases-of-matter/		
Deadline: 5/29	· · · · · ·	· · · · · · ·

Lightning review of bot time
Given - extended unitary (2+1)-dim TQFT Z
- a "self-dual color" X (secretly, a self-dual doject
in unitary modular tensor category determined by 2) - two planar matchings TiS of 2k points
such $+4+$ :
- quatum representation
$Z: B_{4k} \rightarrow U(Z(4k; X_1))$
- IT>, IS> linearly independent in 2 (2t; X, I)

then: Can "lift" quatum circuit C (over founde universal gate set) acting on n qubits to a braid diagram be E Bank such that be acts on subspace  $H_k \otimes H_k \otimes \cdots \otimes H_k \leq 2 (\lambda_n k; X_1),$ where  $H_{k} = spon\{T, IS\}$ , in the same way Moreover, For the isomorphism In Hk identifies Concretenes, We Use  $|0\rangle = \frac{1}{\sqrt{\tau}}$  $\sqrt{\langle T | T \rangle} / T = U U U$ 

Ьĸ  $\times \times$ XXXXX ×  $\bigcup (\mathbb{C}^{2} \otimes \mathbb{C}^{2})$  $g_{1}h_{1}h_{\epsilon} \in \mathcal{H}_{4}($  $b_{3}, b_{5}, b_{k} \in \mathcal{B}_{8}$ 

The encoding CH? bc is linear time.
We might call this topological quatum computing L/c circuits can be encoded inside a TQFT
However, there's an even better reason to call it TQC: if we are using C to answer a Yes/No question, then the probability of a Yes outcome is closely
related to X-colored link invariant of bc "closed up" with copies of T.

la part: to questi	cular, we on asked a	call ;+ TQC t ad of f	E b/c F t	he answer we	e how give
1-10~	20	topo	log:cal	inver:	乄
of	Knots	/ links	13-4	naitol	S
deriv	ied	From	2 re	late te	
this	mod	e) é	fom	putat:o	ر ب

I. "Accept probability of circuit" = "Normalized quantum invariat"
Notice we haven't actually used the identity
$l_{n} $ $\sim $ $(\tau)$
$\frac{10}{\sqrt{2}} = \frac{10}{\sqrt{2}}$
· · · · · · · · · · · · · · · · · · ·
Here's why it matters.
$\langle 000  C   000 \rangle = \langle TTT  L_C   TTT \rangle$
<pre></pre> <pre>&lt;</pre>
and numerator and demonstrator of RHS both have
topological interpretation, thanks to TQFT axioms.

<TT ... T/6c/TT --- T> = 2(6c) where 6c X-colored link diagram as follows: vibbon  $\langle T | \otimes \langle T | \otimes \cdots \otimes \langle T |$  $|T\rangle \otimes |T\rangle \otimes \cdots \otimes |T\rangle$ 



2(K, UK2) = 2(K).2(K) EBZK  $(\langle T | T \rangle)^n = (\langle T | | J | T \rangle)^n = 2(O^k)^n = 2(O_x)^{nk}$ where Ox is X-colored Unknot and Ox is X-colored Unlink w/ K-components.

Thus,  $\langle 00-0|C|00-0\rangle = 2(\hat{b}_{c})$  $Z(O_{v})^{nk}$ Example: Jones-Kauttman TQFT 4/ C= Ugsly-used, X=V the defining correspondation of Ugsl2, and q = elni/k, then 2(6c) is value of Jones polynomial of 6c at q1 ad  $2(O_{y}) = q + q^{-1}$  $e^{2\pi i/100} + e^{-2\pi i/100} = (-\epsilon)$ 

Reminder: BQP (29, 1/3) 21: gate st
Decision problem $F: \{0,1\}^* \rightarrow \{0,1\} = \{N_0, Y_{es}\}$ is in BRP iF:
exists a classical poly time algorithm that converts bit string $x \in \{011\}^n$ to a $Z = circuit$ $C_x$ such that $\langle F(x), x, 0^{m-1}   C_x   x, 0^m \rangle \ge \frac{2}{3}$ .
Note: here I'm letting $C_X$ depend on $X_1$ and not just $ X  = n$ .

$\frac{Variation}{\mathcal{L}: gate} : BQP(\mathcal{B}, \frac{1}{3})$
Decision problem $F: \{0,1\}^* \rightarrow \{0,1\} = \{N_0, Y_{es}\}$ is in BRP iF:
exists a classical poly time algorithm that converts bit string $x \in \{011\}^n$ to a $21 = circuit$ $C_x$ such that $\langle \overline{F(x)}, 0^n, 0^{m-1}   C_x   0^n, 0^m \rangle \ge \frac{2}{3}$ .
So: We might as well allow x to prepare x From 000. We negate FTX) For contrived resson.

	• • • •		 	
±(x)	0 0 0		 	
Wort I L L			 	
· · · · · · · · · · · · · · · · · · ·			 	
$\Gamma(\chi) = \Gamma(\chi) + $			 	
(x, x, x, x) 000			 	
	· · • • · · ·		 	
	11	$\sqrt{2}$	 	
		x - 0 / /	 	
X, x, 3 000			 	
and had ancillas			 	
	0 0 0 0		 	
	• • • •		 	
	• • • •		 	
	0 0 0 0		 	
	• • • •		 	
	• • • •		 	
	• • • •		 	
	• • • •		 	

A reference:

**Proposition 2.3.**  $D \in BQP$  if and only if there is a quantum circuit C = C(x) with poly(|x|) unitary gates acting on n = poly(|x|) qubits, such that C itself can be generated in deterministic polynomial time FP, and such that the probability

$$p(x) = |\langle 0^n | C | 0^n \rangle|^2 \tag{2.1}$$

is at least 2/3 if D(x) = yes and at most 1/3 if D(x) is no.

[Kuperberg, "How hard is it to approximate the Jours polynomial?"]

Theorem (Topological quature computing) Suppose 2 and X satisty conditions above. Then the decision problem F: {0,1}\* -> {0,1} = {No, Yes} is in BQP if and only if there exists a polynomial time (classical) algorithm that takes y E { 011} to a braid diagram by such that  $\left[\frac{\frac{2}{2}\left(\tilde{b}_{\gamma}\right)}{\frac{2}{2}\left(O_{\chi}\right)^{n_{k}}}\right]^{2} \frac{2}{3} ; f = F(\gamma) = Yes$ and  $\left[\frac{2(\tilde{b}_{\gamma})}{2(O_{\chi})^{mk}}\right]^{2} = \frac{1}{3}$  if  $F(\gamma) = N_{0}$ .

<u>Remarks</u>
l. Conditions on X can be relaxed (e.g. not self
dual, use multiple colors to build a qubit, etc).
Unclear what precise level at generality ought to be.
2. I don't know examples of Z + X such that
$Z: B_k \rightarrow U(Z(k; X_I))$
has infinite image for all KND BUT
is NEVER dese
· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·

No lavero, 5/c these are two different Hilbert Spaces Instrul, use "color preserving subgroup" B3,3 of B6 

Meeting 14.1: Computational complexity of TQFT invariants								
I. Approximating quantum	invariants	w/ quaturs	computers	•				
I. Bad news.			· · · · · · · · · · · · · · · · ·	•				
				•				
		· · · · · · · · · · · ·	· · · · · · · · · · · · · · · ·	•				
	E	5	· · · · · · · · · · · · · · · · · · ·	•				
INSTRUCTOR + COURSE			· · · · · · · · · · · · · · · · ·	•				
EVALUATION SYSTEM			· · · · · · · · · · · · · · · ·	•				
Planta				•				
$\int  E   E  = 00$	evar.							
Uerd line J 7 0	· · · · · · · · · · · · · · · · · · ·							

I. Approximating quantum invariants w/ quatum computers
$S_{\circ}$ $F_{ac}$ :
- built model(s) of quantum computation using
2+11- dimensional once-extended Unitary TQFTS
- normalited quantum invariants of knots/links are
sometimes "important amplitudes" of quatum circuits
$\langle 00 - 0 C 00 - 0\rangle = 2(\tilde{b}_{c})$ (oristructed From Circuit
$\overline{\zeta(O_{x})^{nk}}$
Note: there are tlavors for closed 3-man: folds (instead of
(inks in >) Using quitur reps of MLG (closed surface)

Natural	question.			
ſs	there	9 <i>"</i> C	onverse	e`?Can
quart	Um Co	mpute	rs do	Something
For	topol	ogy?		
	· · · · · · · · · · · · ·			

Kind of. Suppose we have:	
- once extend unitary TQFT 2 and	color X (not self-dual)
Ten X-colored ribbon link dingram	
Convert L to grantum circuit	×
CL such that	
$\langle 00-0 C_{L}/00-0\rangle = \frac{2(L)}{C_{L}}$	A AV
$\zeta \left( \bigcirc_X \right)^{\circ(L)}$	
where $B(L)$ is the bridge number	Llla 420 from Knot Atlas

More precisely: to "have 2 and X" means ve have: - an identification of Hilbert spaces  $\frac{2}{2}(X_{1}^{\delta}X^{\epsilon}) = \bigoplus_{N \in \Gamma} \frac{2}{2}\left(\underbrace{\begin{array}{c} & & \\ & \chi \\ & & \chi \end{array}\right) \xrightarrow{\simeq} \int_{\Gamma} \frac{N(x^{\epsilon}, x^{\epsilon})}{\sqrt{2}}$ qudits w/  $\mathcal{J} = \mathcal{N} \left( \times^{\mathcal{S}} (X^{\mathcal{E}}) \right)$ where  $d_1 \varepsilon = \phi$  or  $\chi$  such that  $2(x, x^*; 1) \geq \left( \begin{array}{c} x \\ y \end{array} \right) + \left( \begin{array}{c} x \\ y \end{array} \right)$ |0) € ([ N(x, x\*) Normalization Factor = 2 (Or)

- descriptions (e.g. matrices / algebraic entries) of Fraidine gates  $\bigoplus_{y} Z\left( \underbrace{+ x^{\xi} + x^{\xi}}_{y} \right) \xrightarrow{\cong} (N(x^{\xi}, x^{\xi}))$ Graiding  $\bigoplus Z \left( \underbrace{x_{\xi}}_{X_{\xi}} \underbrace{x_{\xi}}_{X_{\xi}} \right) \xrightarrow{\cong} \left( \bigwedge (x^{\xi}, x^{\xi}) \right) \xrightarrow{g_{g_{\xi}}}$ 



 $\bigoplus_{Y} Z\left( \underbrace{+ x^{\epsilon_1} x^{\epsilon_2}}_{X^{\epsilon_1}} \right) Z \left( \underbrace{+ x^{\epsilon_2} x^{\epsilon_2}}_{X^{\epsilon_1}} \right) Z \left( \underbrace{- x^{\epsilon_2} x^{\epsilon_2} x^{\epsilon_2}}_{X^{\epsilon_1}} \right) Z \left( \underbrace{- x^{\epsilon_2} x^{\epsilon_2} x^{\epsilon_2}}_{X^{\epsilon_1}} \right) Z \left( \underbrace{- x^{\epsilon_2} x^{\epsilon_2} x^{\epsilon_2} x^{\epsilon_2}}_{X^{\epsilon_1}} \right) Z \left( \underbrace{- x^{\epsilon_2} x^{\epsilon_2} x^{\epsilon_2} x^{\epsilon_2} x^{\epsilon_2} x^{\epsilon_2}}_{X^{\epsilon_1}} \right) Z \left( \underbrace{- x^{\epsilon_2} x$ binary braiding gate 

Note: the above local data should be considered as (part of)
a combinatorial/finite algebraic definition of TRFT Z.
It needs to satisfy various compatibility conditions
IF we wated to be more precise, should use an
skeletalization of a
Unitary modular tensor
Category.

Converting L to CL: 1. Put L in "standard bridge position" Arrows way



3. Enc	cy to check using TQ	lFT exious
	<b>〈</b> 000/C <sub>L</sub> /000〉=	$= \frac{2(L)}{2(Q_{\chi})^{6(L)}}$
· · · · · · · · ·	where $b(L)$ is the b	ridge number
	of diagram L.	
· · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	

Now what?
We can approximate the protability
<000/CL/000>/2
in usual way via repeated trials. In particular, given
No can Find N-bit binany approximation in O (log N).
$Suppose \left[ P - \left  \left( 00 - 0 \right) C_{L} \right  00 - 0 \right] \right] \leq \varepsilon.$
$T_{Le} \left( P - \left( \frac{2(L)}{2(Q_X)^{5(L)}} \right)^2 \right)^2 \leq \varepsilon$
$\Rightarrow \left  P \cdot \left  \frac{2}{x} \left( \frac{\pi}{2} \right)^{2b(L)} - \left  \frac{2}{(L)} \right ^{2} \right  L \in \left( \frac{\pi}{2} \right) \right ^{2b(L)}$

Now chat? What to compute an invoriant of L. 1100  $\langle 00 - 0|C_{L}|00 - 0\rangle = \frac{2(L)}{2(O_{X})^{b(L)}} u^{b(t)} u^{b(t)}$   $Z(O_{X})^{b(L)} L^{b(L)}$   $L = L^{b(t)} u^{b(t)}$   $L = L^{b(t)} u^{b(t)$ Sol LHS is NOT invoiat. (f(r))

Summerizing : Extracting on invariant of L/ manualy, [Z(L)]~ From the identity  $\langle 00-0|C_{L}|00-0\rangle = 2(L)$  $\frac{2}{2} \left( \bigcirc \right)^{b(L)}$ his error that scales exponentially badly w) b(L). Error depuds on diggram
$\left P\cdot\left \frac{2}{x}\left(\frac{D}{x}\right)^{2b(L)}\right  - \left \frac{2}{2}(L)\right ^{2}\right  \leq \varepsilon \cdot \left \frac{2}{x}\left(\frac{D}{x}\right)\right ^{2b(L)}$
$ f   \frac{1}{x} (O)  \frac{1}{x} $ , we're happy.
But this NEVER happens unless X is on abelian anyon in which case 7(1).
trivial. Moral: iF L is Wide, it takes a to of
work to avercance the error.

Con we rescue any thing? 1. IF we restricted L to 6(L) 4/00, we can compute 2(L) in linear time on a classical computer! No dice! L. (an ve massage L to make b(L) small? For every N70, exists lint L such that b(D) > N for all diagrams D of L.

3. Can une missage CL t- get 9 thinner circuit C'L that is use folo Freedman, Cui-Freedman - Way "Complexity Classes as Mathematical Axions

2. Bond News

Z any TQFT w/ X=X\* al dence **Theorem 1.2.** Let V(L,t) be the Jones polynomial of a link 1 air L described by a link diagram, and let t be a principal, non-9 62 lattice root of unity. Let 0 < a < b be two positive real numbers, and assume as a promise that either |V(L,t)| < a or |V(L,t)| > b. Then it is #P-hard, in the sense of Cook-Turing reduction, to decide which inequality holds. Moreover, it is still #P-hard when L is a knot. (Kupperbry, "How had is it to approximate...? 2(L) 69 or 12(L) / 26 NP-had (even better, #P-had) to distingersh.

Proot Post BQP = "Linear circuits" Aaro-con PP