Microsoft

Fiber Bundle Codes (and Products More Generally), QIP 2021

- M. B. Hastings , J. Haah, R. O'Donnell
- 2/2021

We’re meeting virtually at QIP. 2020 was an eventful year.

Especially eventful for quantum LDPC codes. Distance Record over time:

- $N^{1/2}$ toric code, Kitaev 1997
- $N^{1/2}\ \log(N)^{1/4}$ Freedman, Mayer, Luo 2002
- $N^{1/2}\ \log(N)$ Evra, Kaufman, Zemor 2020 (decodable up to $N^{1/2}\ \log(N)^{1/2}$)
- $N^{1/2}\ \log(N)^{k}$ for any k, Kaufman, Tessler 2020
- $N^{3/5}$ up to polylogs, HHO (one-sided decodable, conjectured two-sided)
- N/log(N), Panteleev, Kalachev, 2020
- $N^{3/5}$ Breuckman, Eberhardt (derandomization of HHO, improved parameters using trick of PK to prove distance)

This talk:

- Explain what a quantum LDPC code is and compare to classical codes
- Explain the idea of “products” and more generally “twisted products” which are involved in all of these constructions
- Talk a bit about the specific constructions

LDPC (quantum) codes and “Good Codes”

Throughout this talk, by “quantum code”, I mean a CSS stabilizer code.

[[n,k,d]] code has n qubits, k logical qubits, distance d.

Non-CSS stabilizer codes can be turned into CSS stabilizer codes (Bravyi, Leemhuis, Terhal). Map [[n,k,d]] -> [[4n, 2k, 2d]] CSS code.

Why LDPC and why stabilizer?
Essential for fault tolerance!

LDPC code (low-density parity check) means all stabilizer weights are O(1). Also, only O(1) stabilizers acting on any qubit.

This allows short quantum circuits to measure stabilizers in O(1) rounds.

There are subsystem codes (Bacon et al) with almost linear distance, but stabilizers are product of many generators. Not suitable for fault tolerance!

Classical LDPC Codes

- Classical codes defined by sparse parity check matrix
- LDPC helps with decoding these codes. Concerns about “short circuits” don’t matter here.
- “Good LDPC codes” exist. [n,k,d]=[n,$\Theta(n), \Theta(n)$]
- In fact, it’s “easy” to write them down. Write down a random sparse parity check matrix and you’ve probably done it!!

Quantum LDPC codes

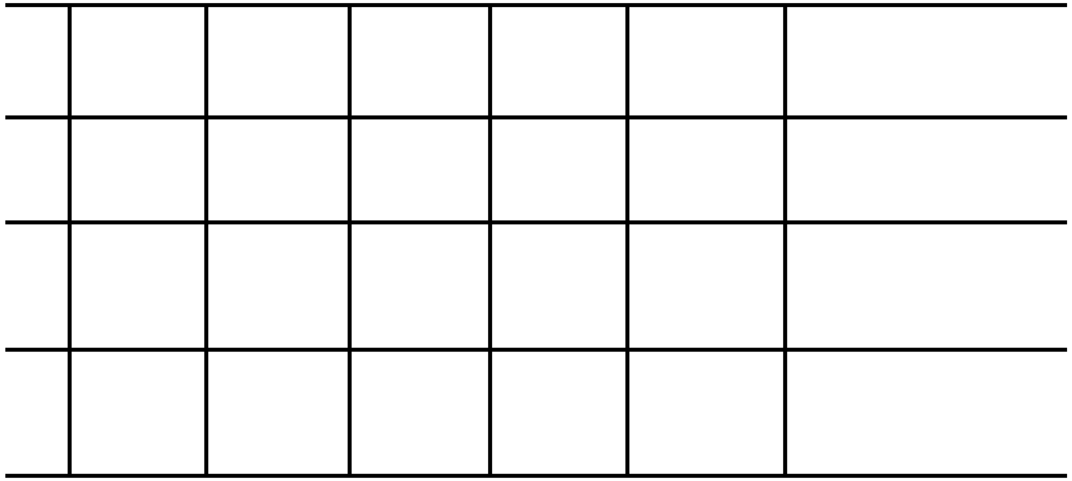
- Not so easy to write down. X and Z stabilizers need to commute. A random choice of X stabilizers will probably have no low weight Z stabilizers that commute with it.
- Hard to achieve high distance. Until mid-2020, the record was

$$d = \Theta(\sqrt{n} \log(n)^c)$$

First code to achieve distance n^c for c>1/2: fiber bundle codes. Further rapid progress afterwards.

Products

Recall the toric code:



Each edge is a qubit

Each vertex is a stabilizer XXXX

Each plaquette is a stabilizer ZZZZ

Torus T^2 is a product of two circles S^1.
Similarly, the toric code can be viewed as a product of two classical codes.

Why Products??

It is a way to get commutativity!

- Use all kinds of randomized ideas from coding theory, and let the products introduce enough structure for a quantum code.

Chain complexes

- Sequence of vector spaces and linear maps between them, called “boundary operators”, ∂_j
- ….$\rightarrow A_{j+1} \rightarrow A_j \rightarrow A_{j-1} \rightarrow \cdots$
- Square of boundary operator equals 0 by definition: $\partial^2 = 0$
- Chain complex over F_2 defines a quantum code. Three spaces in sequence are Z-stabilizers, qubits, X-stabilizers. Stabilizer commute iff boundary squares to 0.
- Basis vectors are called “cells”

More about chain complexes

- Logical operator of code: Z-type logical operators are products of Pauli Z which commute with X-stabilizers, modulo Z-stabilizers. (and the same with X<->Z interchanged)
- Mathematically this is called "homology" (or co-homology for X).
- "j-chains" are vectors in A_j. "Closed chains" are vectors with vanishing boundary. The space of closed chains modulo boundaries is called H_j, the j-th homology group.

$$H_j = Z_j \,/\, B_j$$

Product of chain complex

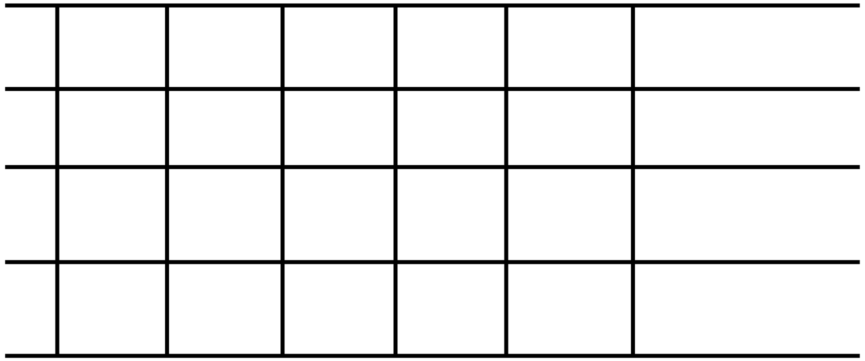
- Cellulation of manifold gives a chain complex (recall toric code).
- It is natural to define new manifolds by products of old ones.
- You can do the same thing with chain complexes directly, without introducing the manifolds.
- $C = A \otimes B$

$$C_j = \bigoplus_k A_k \otimes B_{j-k}$$

$$\partial^C = \partial^A \otimes I \pm I \otimes \partial^B$$

We don’t need to worry about the sign

Toric code as a product



- Chain complex is a product of two “two term” chain complexes
- A,B are both cellulations of a circle.
- Classical codes with stabilizers $Z_i Z_{i+1}$ where i is periodic with period L
- “Horizontal 1-cells” and “Vertical 1-cells” are different terms in sum for $C_1 = A_1 \otimes B_0 \oplus A_0 \otimes B_1$
- Homology can be computed with Kunneth formula (works for any product):

$$\mathrm{H_j(C)} = \oplus_k H_k(A) \otimes H_{j-k}(B)$$

First homology: logical qubits. Zeroth (co)homology: redundant stabilizers.

Early applications of products:

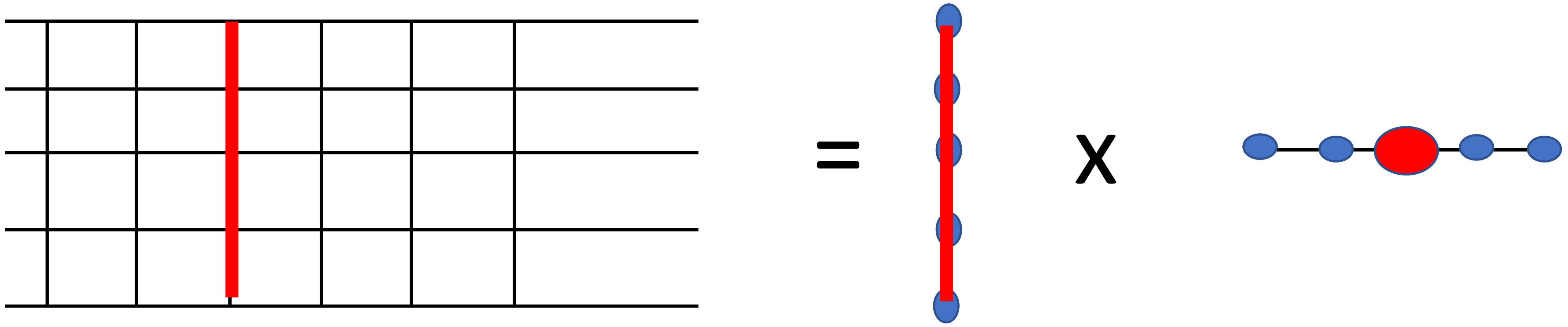
- Homological product codes (good quantum codes, sqrt weight stabilizers), Bravyi-Hastings
- Hypergraph product codes. Take A and B to be chain complexes for a good classical LDPC codes and dual of a good classical LDPC code, respectively. Tillich-Zemor.

By Kunneth, hypergraph product codes have linear rate.

What about distance of those codes???

Distance and Kunneth

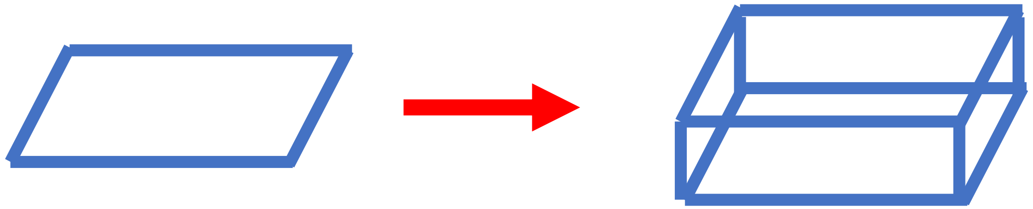
Form representative of j-th homology by product of representatives.



This gives an upper bound to distance in terms of "distances" of input complexes. The quotes are there because it depends on distances for H_1 and H_0 .

Turns out that this bound is tight for hypergraph product codes: square-root distance.

Distance balancing



- Indeed, quite generally we can make the Kunneth bound tight when taking product with a classical code.
- Application: distance balancing (Hastings, 2016; Evra, Kaufman, Zemor 2020 rate improved)
- Input is [[n,k,d_x, d_z]] code. Suppose $d_x > d_z$. Take product with classical code (or its dual) to increase d_z to $d_x = d$.
- Output is $[[n\ \Theta\left(\frac{d_x}{d_z}\right), k\ \Theta\left(\frac{d_x}{d_z}\right), d]]$ code
- Indeed, hypergraph product codes can be understood as distance balancing a classical code which has $d_x = \Theta(n), d_z = 1$

Whenever $d_x d_z \gg N$, it distance balances to >> square-root distance code

Twisted Products

- The inspiration for products of codes comes from topology.
- But topologists know a lot of things more general than products, so why stop there??
- Fiber bundles! “Look like a product locally, but not globally”

By en:User:Musical Linguist - Transwikied from English Wikipedia; originally uploaded there by en:User:Musical Linguist, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=1472591

Example of a fiber bundle: Mobius strip

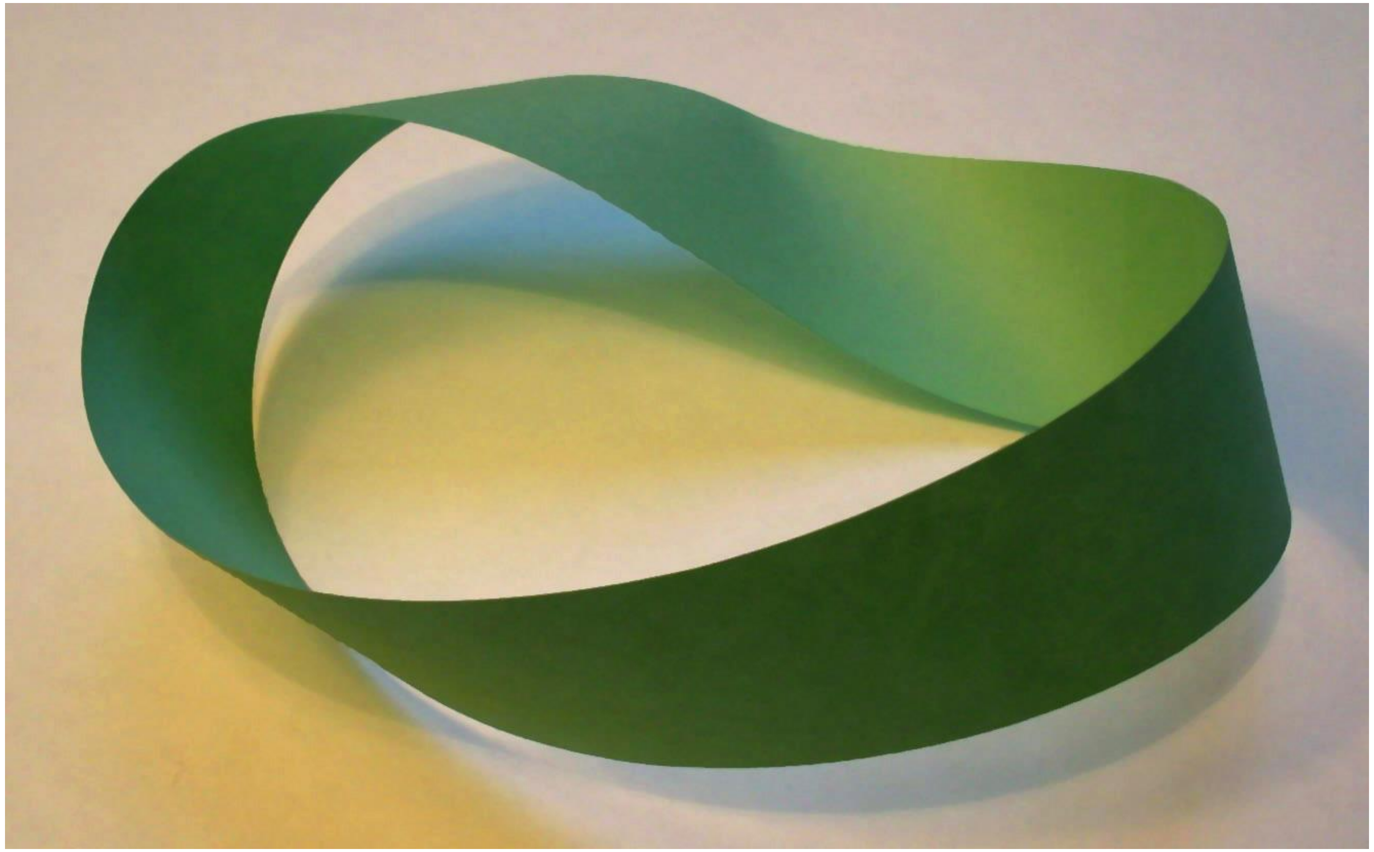


Image By David Benbennick - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=50359

Given by "twisted product" of circle and interval.

Locally it looks like $S^1 x\ I$. But going around circle reflects interval.

Circle is called "**base**". Interval is called "**fiber**".

Product is called "total space". Usually denoted E. $E = B \otimes F$ locally but not globally.

Mobius strip has a “flat connection”. No curvature. That’s what we will care about for codes. But for fun, here is a case with curvature:

Hopf Fibration. The pure states of a single qubit.

Total space is S^3. $(\psi_1,\psi_2), |\psi_1|^2+|\psi_2|^2=1$

Base space is S^2. $\langle\psi|\,\vec{\sigma}\,|\,\psi\rangle$

Fiber is S^1. This is the phase.

But, the total space is not just a product of “direction spin is pointing” and “phase”, even though locally it is.

Twisted product of chain complexes:

- Same choice of cells as in regular product, but we change the boundary operator. No longer just $\partial^E = I \otimes \partial^F + \partial^B \otimes I$

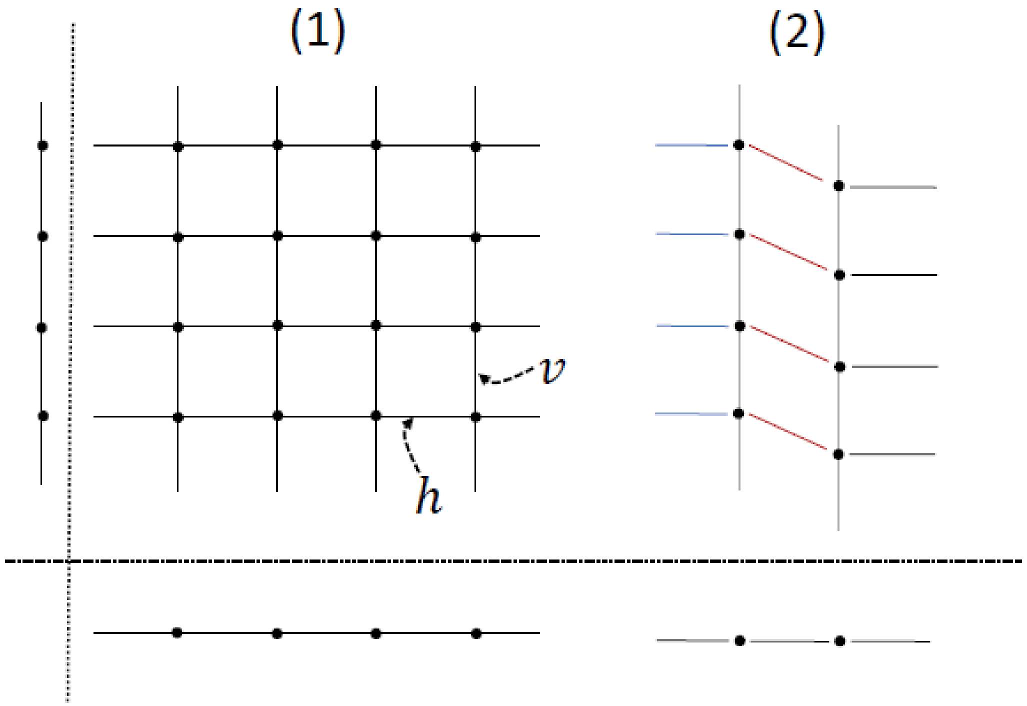
$$\partial^{\mathcal{E}}_{(0,q)}(b^0 \otimes f) = b^0 \otimes \partial f,$$

$$\partial^{\mathcal{E}}_{(1,q)}(b^1 \otimes f) = b^1 \otimes \partial f \ + \sum_{a^0 \in \partial b^1} a^0 \otimes \varphi(b^1, a^0) f.$$

$\phi(b, a)$ is an automorphism (i.e., symmetry) of the fiber

We are giving here the case of no curvature, when B and F are two term complexes. More general possible.

Example: twist of a torus



Twist shown in red.

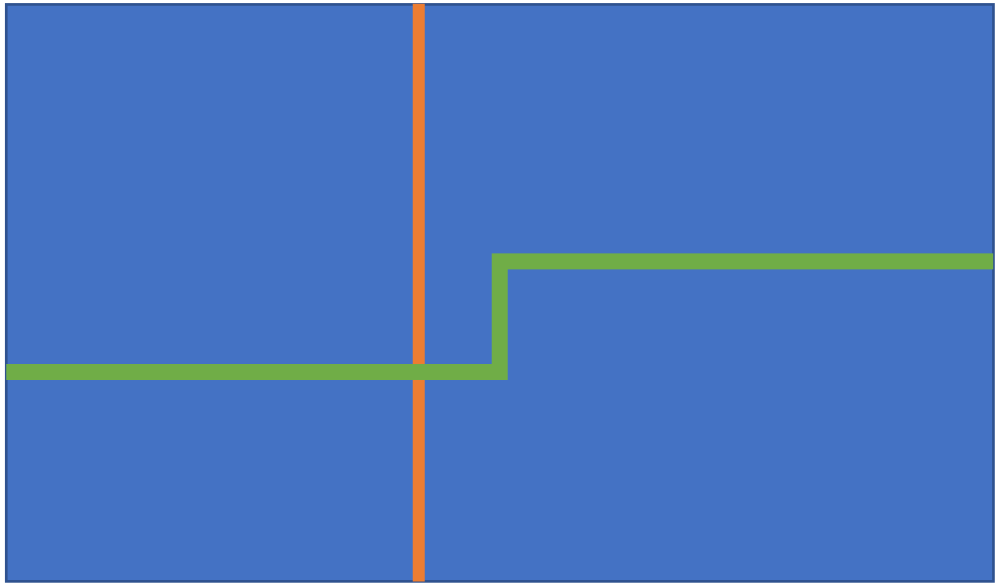
Fiber periodic from top to bottom (i.e., it is a circle).

Automorphism of fiber is just a rotation.

Gauge redundancy: we can “move the twist around”.

Twist of a torus

Using twists, one can improve the distance of the toric code from $\sqrt{N/2}$, by constant factor.



Attach top to bottom.
Attach left to right with a twist.

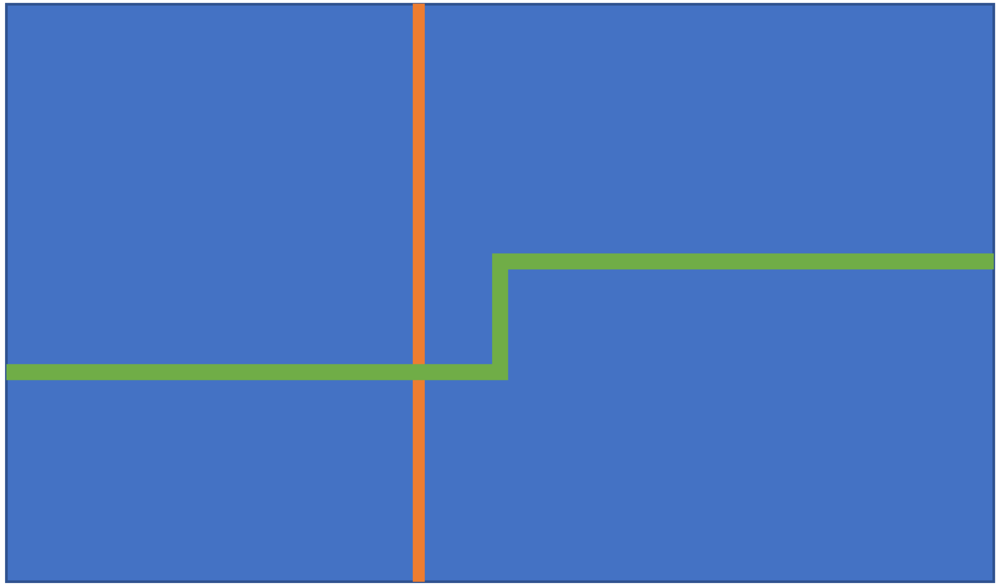
Shortest path from top to bottom same.
Shortest from left to right increases weight.
Kunneth formula no longer gives representatives.

All the various constructions (HHO, PK, BE)

- These are all fiber bundles where the fiber is a circle (nice choice with automorphism being rotation). We will ignore the possibility of reflections.
- We'll give a unified picture later, explaining why it's all a "circle bundle".
- Remark: PK gave distance rate tradeoffs $[[N, N^{\alpha}, N^{1-\frac{\alpha}{2}}]]$ up to constants. Using a trick that they found, we can see that the HHO codes actually hit this line too, for smaller range of alpha, up to polylogs.

Circle bundle with base as classical code

- HHO construction has random classical code as base (polylog weight, later reduced to O(1)). It has random twists with circle as fiber.



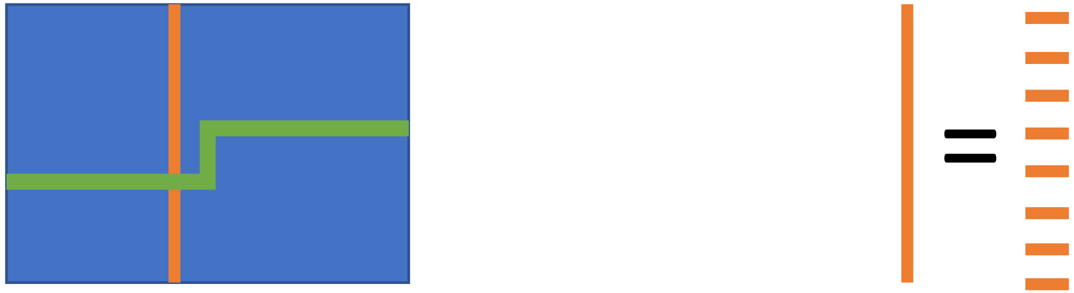
There will be n_F bits in the fiber. n_B bits in the base.

That “vertical line” still has weight n_F.

That “horizontal” line now has more weight. The “endpoint” shifts a distance in fiber and the weight of the endpoint is now of order n_F also! This is because anything far from codeword in base violates lots of checks.

Cohomology distance (and decoder)

“Cohomology” distance. Weight of lowest cohomology rep (distance against X error). This is the vertical line.



- There is still a Kunneth-like formula that says that the whole vertical line times a point in the base is a representative.
- Other representatives given by adding boundaries.
- Expansion properties of base prove that that can’t reduce weight. Reducing weight in one place makes it worse in more places. Distance of order n_F
- This actually gives an efficient decoding algorithm up to some constant fraction of d_X that starts with a guess with few base cells and then greedily adds boundaries

Homology distance intuition

- When you project out the fiber, you must have a nontrivial word of base code, hence horizontal weight $\Omega(n_B)$since base is good
- Base expands, so endpoint has weight $\Omega(n_B)$ also.
- Actually this relies on stronger expansion properties than just the base. We called it “twist graph code”, same as expansion of “lift” in other terminology.
- We used a trick (choosing twists multiple of $\sqrt{n_B}$) to lower bound homology weight by $n_F\sqrt{n_B}$
- This gave final distance. Actually a trick of PK carries over to our code and shows it should be $n_F n_B$ giving a tighter bound.

Unified picture

- Several different twisted products: fiber bundle (HHO), lifted product (PK), balanced product (BE). Current realizations all are circle bundles.
- Fiber bundle over base can be described as product of universal cover of base times fiber, modulo symmetries
- Symmetry of form: lift of a nontrivial closed path in base times symmetry in fiber.

Image By David Benbennick - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=50359

Circle is real line modulo “translate by 1”.

Real line times interval modulo “translate by 1 and flip interval”.

Unified picture

- Fiber bundle over base can be described as product of universal cover of base times fiber, modulo symmetries
- Universal cover is infinite. In fact, we can take a finite cover of the base and still mod out.
- Product mod symmetry is balanced product.

Image By David Benbennick - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=50359

Circle is interval [0,2] modulo "translate by 1".

[0,2] times interval modulo "translate by 1 and flip interval".

If first complex in balanced product is two term and free action, then it is bundle (base is first complex mod symmetry). If second has this property too, it is lifted product. (see BE)

What now?

- Twisted products very useful for forming high distance LDPC quantum codes
- Can we attain linear distance? Can we attain “good” codes with linear distance and nonzero rate?
- Can we decode these codes? (one-sided decoding proven for HHO, two-sided conjectured)
- Bundles with non-flat connection?
- Applications to mathematics: “turning codes back into manifolds”, Freedman-Hastings 2020
- Practical applications?

Microsoft

Thank you.