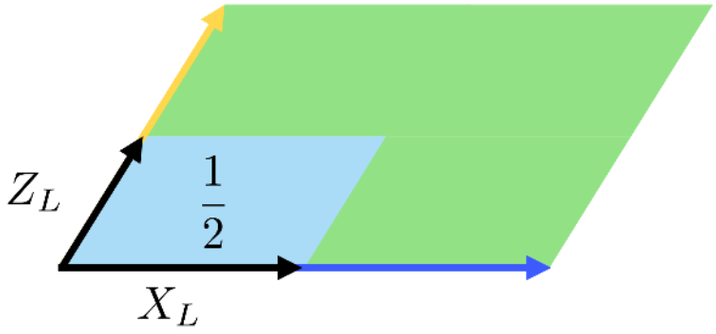
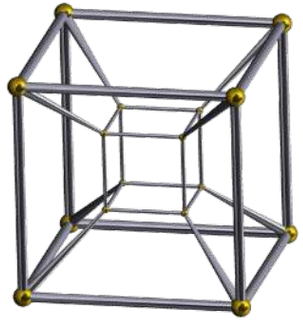
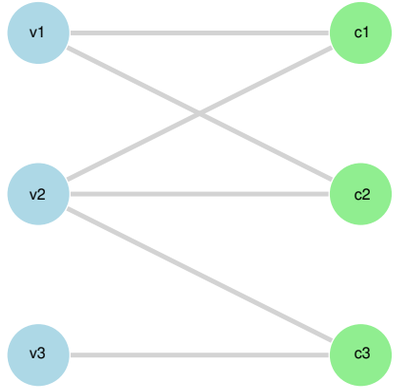
GKP codes with generalized concatenation or none at all







Francesco Arzani

Inria | ENS | PSL

Quantum

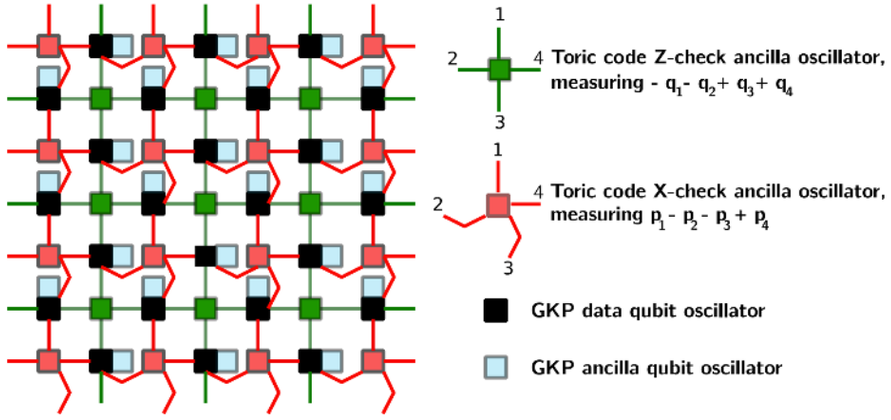
Architectures,
Algorithms,
Applications

and their **T**heory

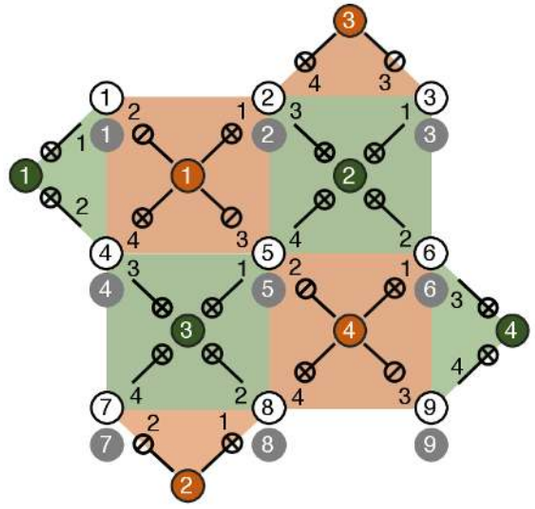
QAT

Continuous variables, MBQC, Q Machine Learning, verification, crypto, ...

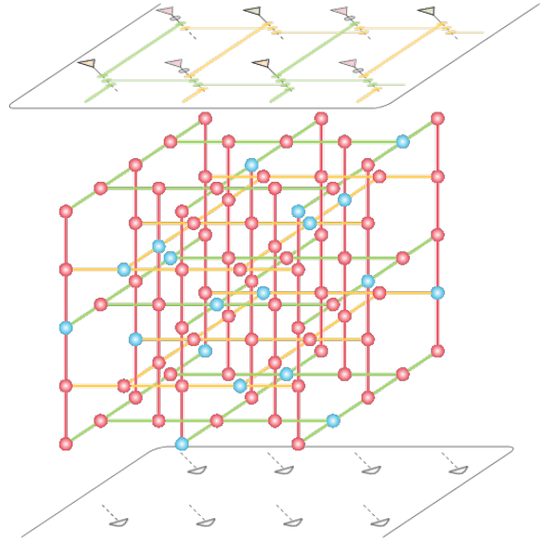
> **The goal:** GKP codes without concatenation!
> But…**why?** Don't you like concatenation?
> It's great!



Vuillot et al, PRA (2019)



Noh & Chamberland, PRA (2020)



Bourassa et al, Quantum (2021)

Because it's very structured → Is it optimal?

Is it *close to* optimal?

Previous work (not exhaustive)

PHYSICAL REVIEW A, VOLUME 64, 062301

Achievable rates for the Gaussian quantum channel

Jim Harrington* and John Preskill†
Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125
(Received 17 May 2001; published 8 November 2001)

PRX QUANTUM **3,** 010335 (2022)

Encoding Qubits in Multimode Grid States

Baptiste Royer,[1,2,*] Shraddha Singh,[2,3] and S.M. Girvin[1,2]

Quantum
the open journal for quantum science

Gottesman-Kitaev-Preskill codes: A lattice perspective

Jonathan Conrad[1,2], Jens Eisert[1,2], and Francesco Arzani[1]

PRX QUANTUM **4,** 040334 (2023)

Closest Lattice Point Decoding for Multimode Gottesman-Kitaev-Preskill Codes

Mao Lin,[1,*] Christopher Chamberland,[2,3] and Kyungjoo Noh[2,3]

Quantum
the open journal for quantum science

Good Gottesman-Kitaev-Preskill codes from the NTRU cryptosystem

Jonathan Conrad[1,2], Jens Eisert[1,2,3], and Jean-Pierre Seifert[4,5]

And many more…

Outline

1) Gottesman-Kitaev-Preskill codes

2) Generalized concatenation: multi-mode inner codes
   with Florian Cottier

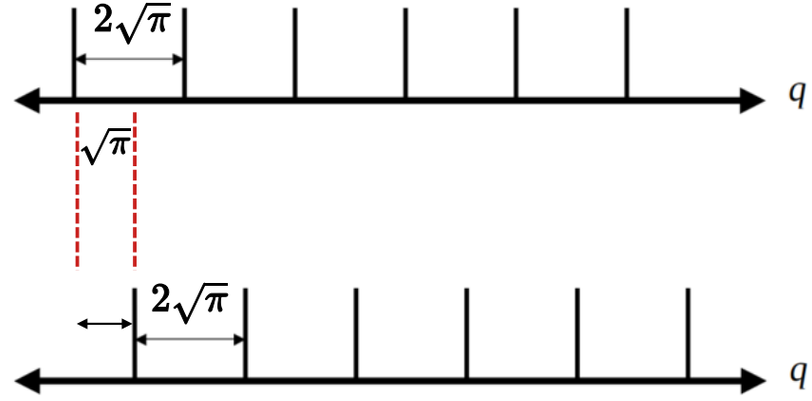
3) Quantum low-density lattice codes (qLDLCs)
   with Timo Hillmann

Part 1 : GKP codes

Square GKP qubits

$$|0_{\mathrm{L}}\rangle = \sum_{k=-\infty}^{\infty} \left|2k\sqrt{\pi}\right\rangle_q = \sum_{k=-\infty}^{\infty} \left|k\sqrt{\pi}\right\rangle_p$$

$$|1_{\mathrm{L}}\rangle = \sum_{k=-\infty}^{\infty} \left|(2k+1)\sqrt{\pi}\right\rangle_q = \sum_{k=-\infty}^{\infty} (-1)^k \left|k\sqrt{\pi}\right\rangle_p$$

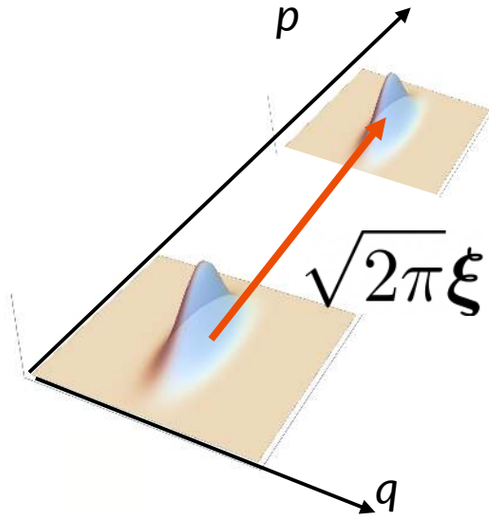


$$e^{-i2\sqrt{\pi}\hat{p}}|j_l\rangle = e^{i2\sqrt{\pi}\hat{q}}|j_l\rangle = |j_l\rangle$$

Displacement operators

$$D^\dagger(\boldsymbol{\xi})\hat{\boldsymbol{x}}D(\boldsymbol{\xi}) = \hat{\boldsymbol{x}} + \sqrt{2\pi}\boldsymbol{\xi}$$

$$D(\boldsymbol{\xi})D(\boldsymbol{\eta}) = e^{-i2\pi\boldsymbol{\xi}^T J\boldsymbol{\eta}}D(\boldsymbol{\eta})D(\boldsymbol{\xi})$$



Commute up to phase!

$$\hat{\boldsymbol{x}} = (q_1, \ldots, q_n, p_1, \ldots, p_n)^T$$

$$[\hat{x}_j, \hat{x}_k] = iJ_{jk}$$

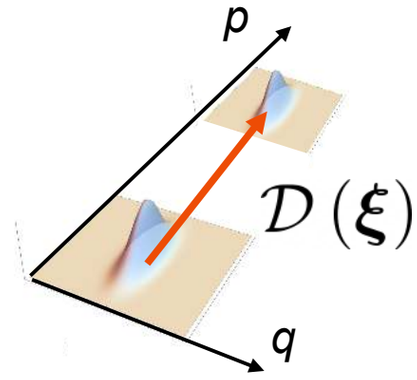
$$J = \begin{pmatrix} \mathbf{0} & \mathbb{I} \\ -\mathbb{I} & \mathbf{0} \end{pmatrix}$$

Generalized GKP codes

Gottesman, Kitaev, Preskill PRA 64 (2001)

$$\{D(\boldsymbol{\xi}_1), \ldots, D(\boldsymbol{\xi}_{2n})\} \Rightarrow \text{Code: } D(\boldsymbol{\xi}_j)|\psi\rangle = |\psi\rangle \quad \forall j$$

$$D(\boldsymbol{\xi}_j)D(\boldsymbol{\xi}_k) = D(\boldsymbol{\xi}_k)D(\boldsymbol{\xi}_j)$$



$$\mathcal{S} = \langle D(\boldsymbol{\xi}_1), \ldots, D(\boldsymbol{\xi}_{2n})\rangle$$

$$D(\boldsymbol{\xi}_j)D(\boldsymbol{\xi}_k) = e^{i\phi_{jk}} D(\boldsymbol{\xi}_j + \boldsymbol{\xi}_k)$$

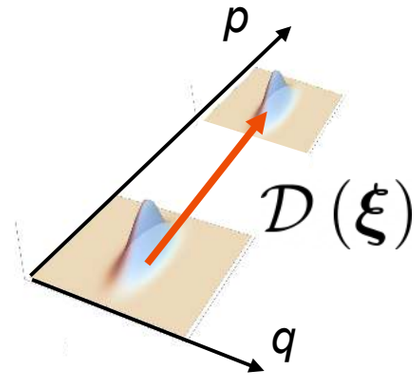
$$\mathcal{S} \cong \mathcal{L} = \{\textstyle\sum_j z_j \boldsymbol{\xi}_j \ : \ z_j \in \mathbb{Z}\}$$

Generalized GKP codes

Gottesman, Kitaev, Preskill PRA 64 (2001)

$$\{D(\boldsymbol{\xi}_1), \ldots, D(\boldsymbol{\xi}_{2n})\} \Rightarrow \text{Code: } D(\boldsymbol{\xi}_j)|\psi\rangle = |\psi\rangle \quad \forall j$$

$$D(\boldsymbol{\xi}_j)D(\boldsymbol{\xi}_k) = D(\boldsymbol{\xi}_k)D(\boldsymbol{\xi}_j)$$



Commutation: $\left[D\left(\boldsymbol{\xi}_j\right), D\left(\boldsymbol{\xi}_j\right)\right] = 0 \Leftrightarrow \boldsymbol{\xi}_j^T J \boldsymbol{\xi}_k \in \mathbb{Z}$

$\boxed{A_{jk}} = \left(MJM^T\right)_{jk} \in \mathbb{Z}$ ⇒ Symplectically integral lattices

Symplectic Gram matrix

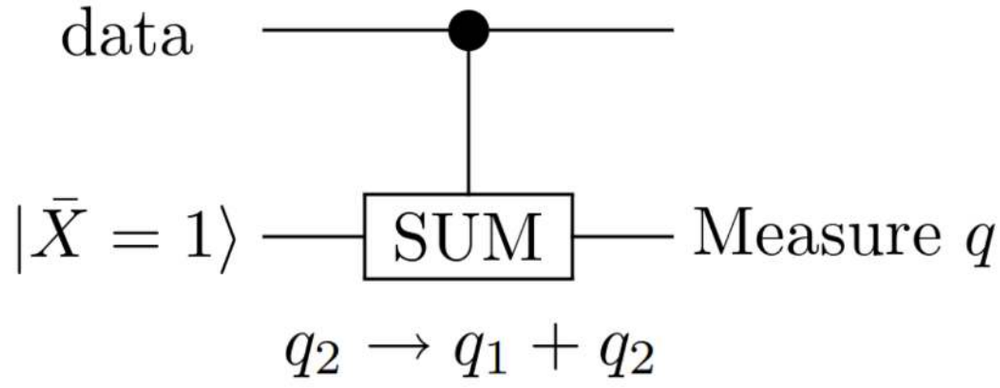
This is the only condition we need!

Syndrome extraction and decoding

$$D\left(M_i^T\right) D\left(\boldsymbol{e}\right) |\psi\rangle = e^{i2\pi M_i J \boldsymbol{e}} D\left(\boldsymbol{e}\right) |\psi\rangle \qquad \boldsymbol{s}(\boldsymbol{e}) = MJ\boldsymbol{e} \mod 1$$

Use encoded ancillas
+ Gaussian operations

Gottesman, Kitaev, Preskill PRA 64 (2001)

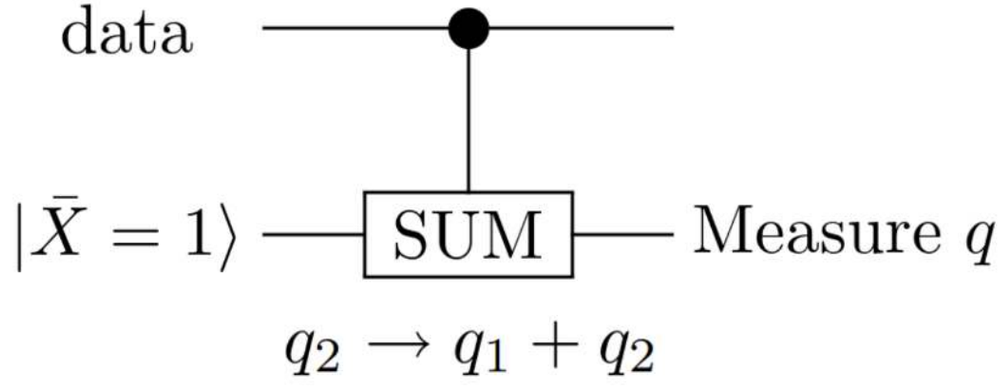


Syndrome extraction and decoding

$$D\left(M_i^T\right) D\left(\boldsymbol{e}\right) |\psi\rangle = e^{i2\pi M_i J \boldsymbol{e}} D\left(\boldsymbol{e}\right) |\psi\rangle \qquad \boldsymbol{s}(\boldsymbol{e}) = MJ\boldsymbol{e} \mod 1$$

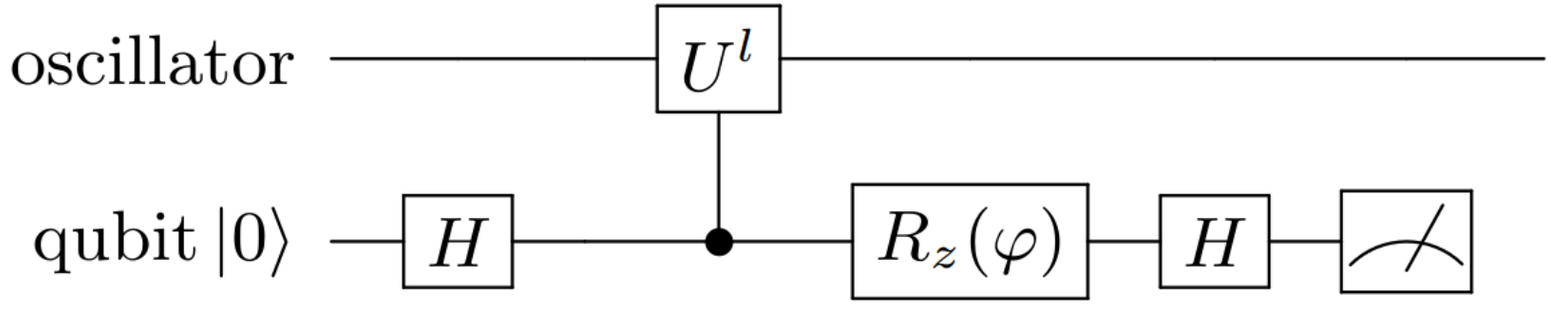
Use encoded ancillas
+ Gaussian operations

Gottesman, Kitaev, Preskill PRA 64 (2001)



Phase estimation
with ancillary qubit

Terhal, Weigand, PRA 93 (2016)



Syndrome extraction and decoding

$$D\left(M_i^T\right) D\left(\boldsymbol{e}\right) |\psi\rangle = e^{i2\pi M_i J \boldsymbol{e}} D\left(\boldsymbol{e}\right) |\psi\rangle \qquad \boldsymbol{s}(\boldsymbol{e}) = MJ\boldsymbol{e} \mod 1$$

$\boldsymbol{\eta}(\boldsymbol{s}) = (MJ)^{-1}\boldsymbol{s}$ returns to codespace… but have we applied logical operation?

$\boldsymbol{MJ}(\boldsymbol{\eta}(\boldsymbol{s}) + \boldsymbol{e}) \in \mathbb{Z}^{2n}$ ⟹ Either applied stabilizer or Pauli

Syndrome extraction and decoding

$$D\left(M_i^T\right) D\left(\boldsymbol{e}\right) |\psi\rangle = e^{i2\pi M_i J \boldsymbol{e}} D\left(\boldsymbol{e}\right) |\psi\rangle \qquad \boldsymbol{s}(\boldsymbol{e}) = MJ\boldsymbol{e} \mod 1$$

$\boldsymbol{\eta}(\boldsymbol{s}) = (MJ)^{-1}\boldsymbol{s}$ returns to codespace… but have we applied logical operation?

Evaluate coset probabilities:

$$P(\boldsymbol{e} + \boldsymbol{\eta}(\boldsymbol{s}) \sim X_L|\boldsymbol{s}) \propto \sum_{\boldsymbol{\xi}\in\mathcal{L}} P_\sigma(\boldsymbol{e} + \boldsymbol{\eta}(\boldsymbol{s}) + \boldsymbol{\xi})$$

Gaussian random noise

$$\mathcal{N}(\rho) \propto \int d^{2n}\boldsymbol{x} e^{-\frac{||\boldsymbol{x}||}{\sigma^2}} D(\boldsymbol{x})\rho D^\dagger(\boldsymbol{x})$$

Maximum-likelihood:

Find most likely logical coset

$\Downarrow \sigma \to 0$

Minimum-energy:

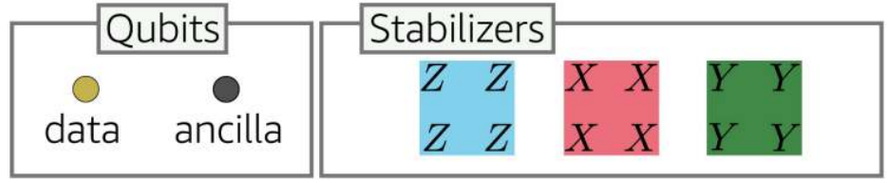
Find most likely *single* term

Essentially ~ closest vector problem
→ NP-Hard for general lattices/bases

Part 2 : concatenation with multi-mode inner codes

With
Florian Cottier

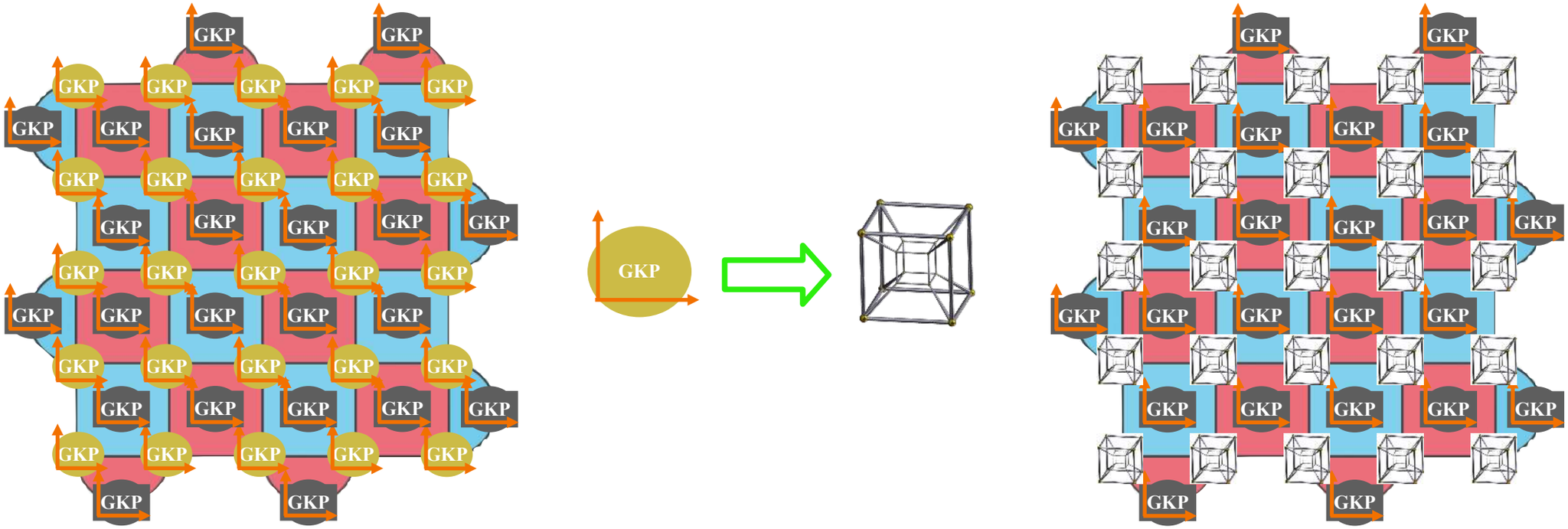
“Generalized” concatenation



Decode in 2 steps:

1. Fix each data subsystem to a GKP qubit (syndrome extraction + CVP)
2. Extract outer-code syndromes and run qubit decoder

“Generalized” concatenation

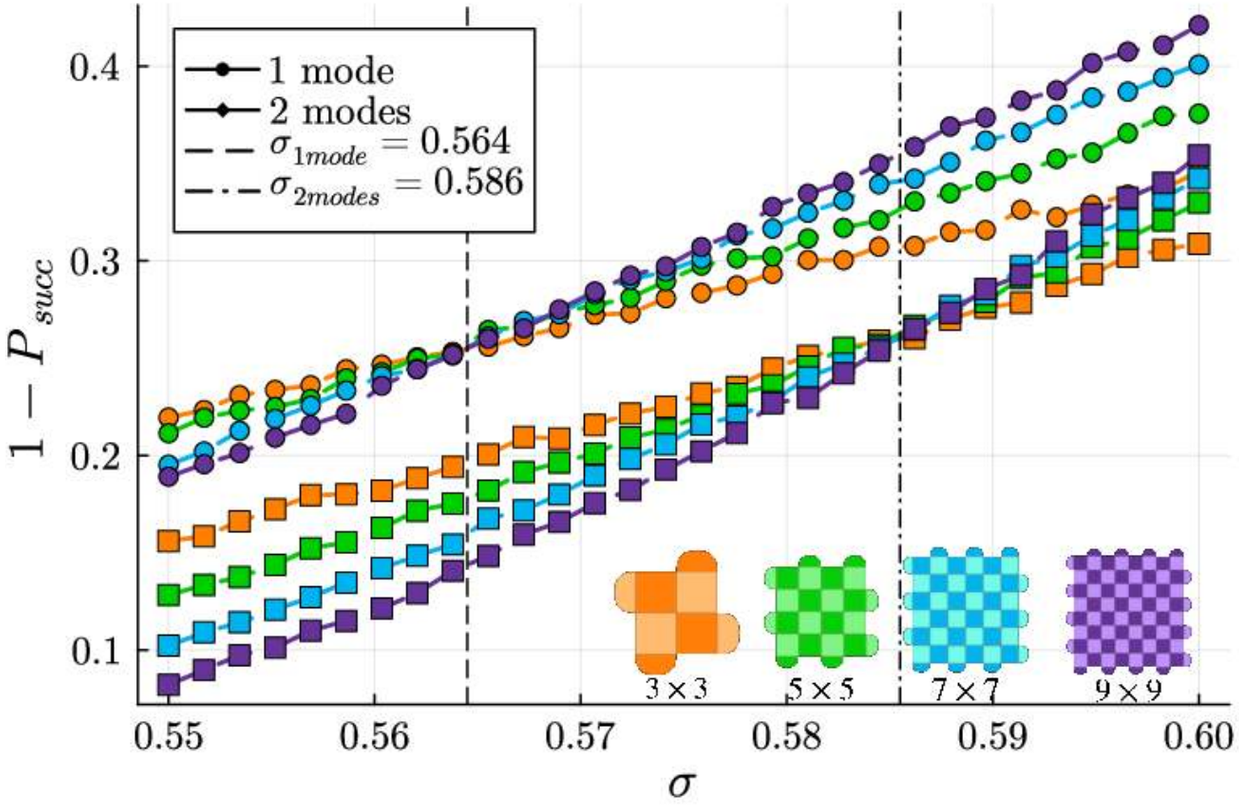


Decode in 2 steps:

1. Fix each data subsystem to a GKP qubit (syndrome extraction + CVP)
2. Extract outer-code syndromes and run qubit decoder

Note: auxiliary modes might be relevant for circuit-level simulations

Code capacity results: 1 vs 2 modes



$\sigma^* \approx 9.63$ dB
(tesseract)

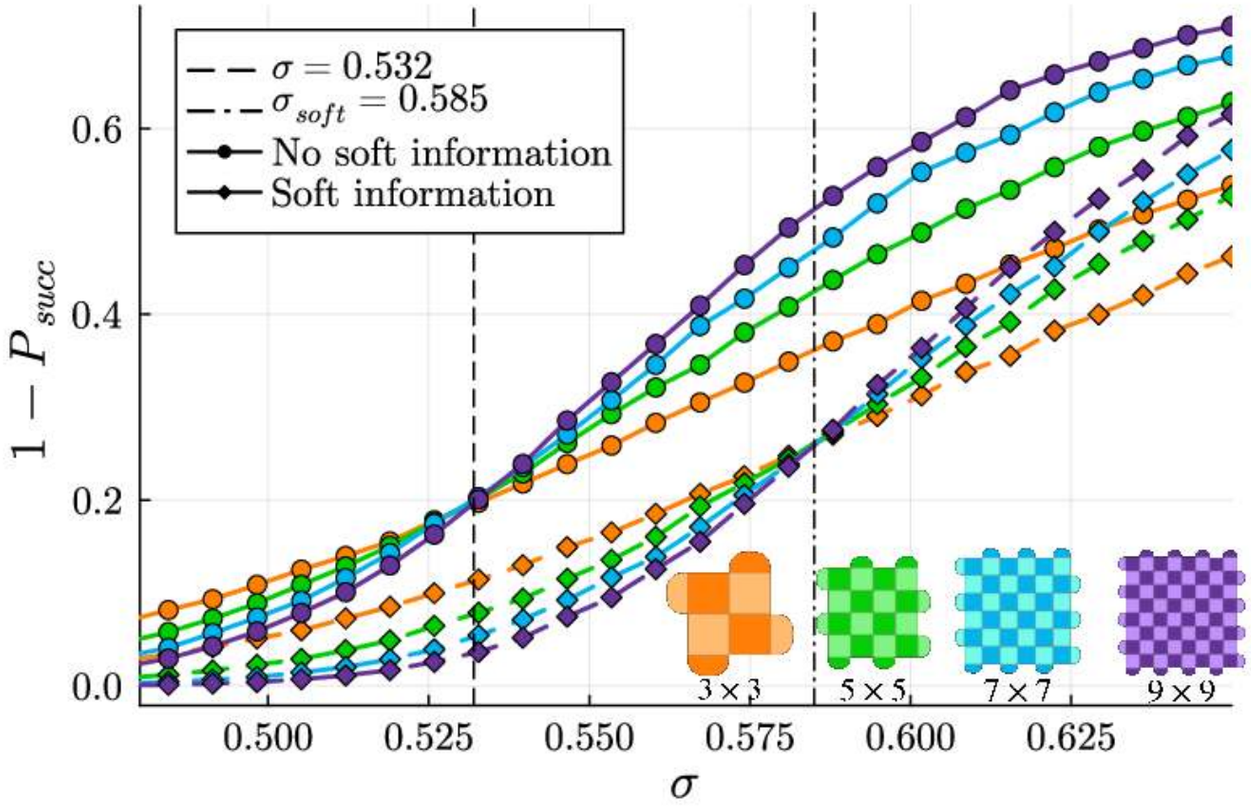
$\sigma^* \approx 9.95$ dB
(Hexagonal)

Compatible with 9.9 dB in

Noh, Chamberland, Brandao PRX Quantum (2022)

But suggests further optimization is possible

Code capacity results: soft information



With soft information

$$\sigma^* \approx 9.63 \text{ dB}$$

Without

$$\sigma^* \approx 10.45 \text{ dB}$$

$$d_X = \min_{b \in \mathbb{Z}^{2N}} \left|\left| e^* + \xi_X - \sqrt{2\pi} M^T b \right|\right|$$

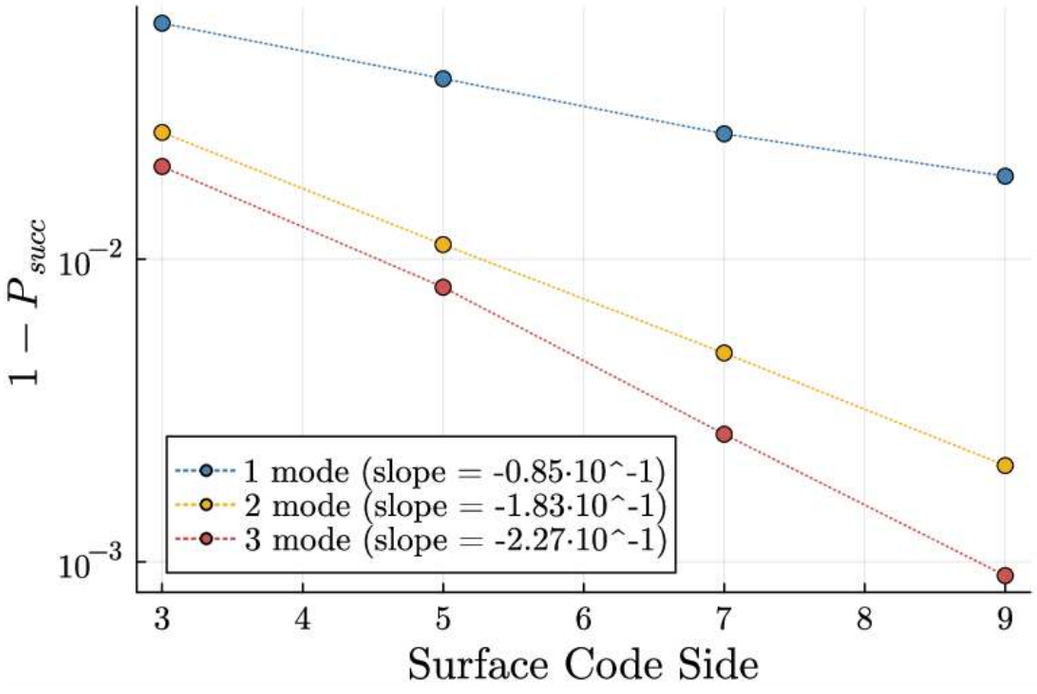
$$\Pr(X|\boldsymbol{s}) \approx P_X = \frac{1}{\sqrt{2\pi\sigma_{gkp}^2}} e^{-{d_X}^2/2\sigma_{gkp}^2}$$

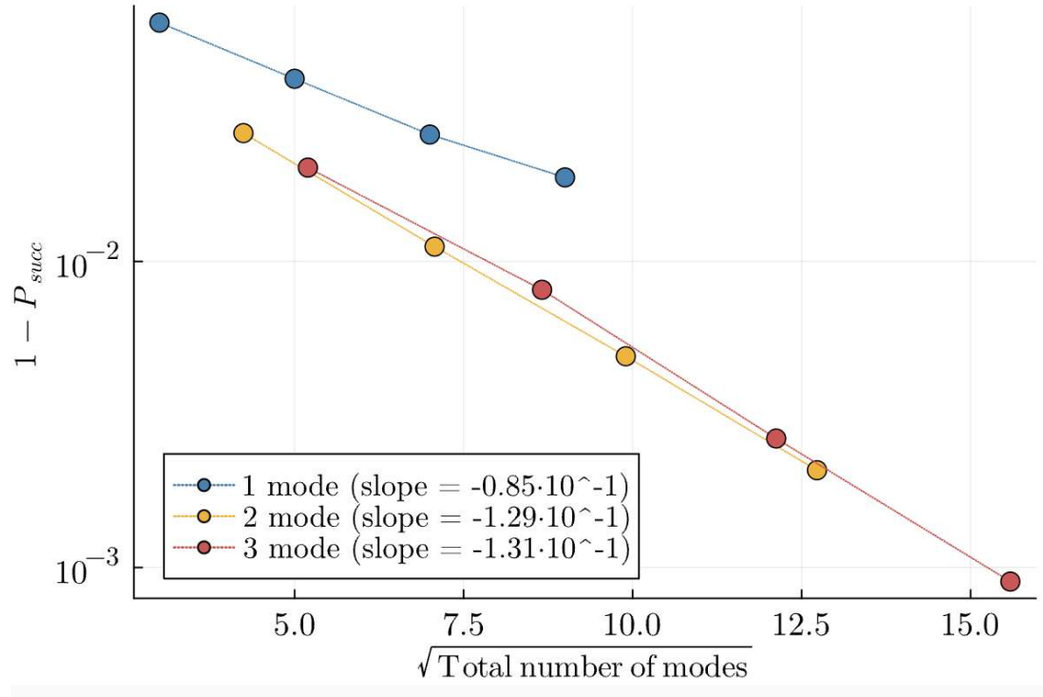
$$L_X = \log \frac{P_I + P_Z}{P_X + P_Y}$$

To pymatching

Code capacity results: subthreshold behaviour

$\sigma = 0.5 \approx 10$ dB





3 modes:

- Similar threshold
- Better sub-threshold*

Sub-threshold is about the same wrt # of modes

Lin, Chamberland, Noh PRX Quantum 4 (2023)

Possibly not optimal?

Part 3 : quantum low-density lattice codes

Low-density lattice codes (LDLCs)

With
Timo Hillmann

Classical lattice codes

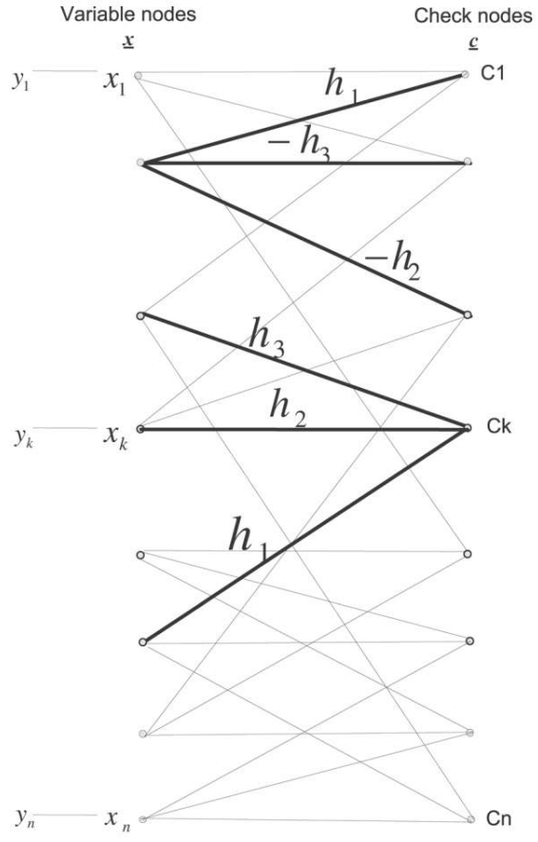
Codewords: $\mathcal{C} = \{x_1, \ldots, x_l\} \subset \mathcal{L} \;\; \Rightarrow Hx_j = 0 \mod 1$

AWGN: $y = x + c, \;\; c \sim \mathcal{N}_\sigma{}^{\otimes n}$

MLD: most likely *x* given *y* $\Leftrightarrow \bar{x} = \mathrm{argmin}_{x \in \mathcal{L}} ||x - y||$

Issues: CVP is NP-hard (in general...)

Solution: find lattices with large distance and "easy" decoding



IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 54, NO. 4, APRIL 2008

Low-Density Lattice Codes

Naftali Sommer, *Senior Member, IEEE*, Meir Feder, *Fellow, IEEE*, and Ofir Shalvi, *Member, IEEE*

Sparsity condition → efficient belief propagation

Belief-propagation for lattice codes

Belief-propagation for lattice codes

1. Initialization : Each variable sends a Gaussian PDF

$$f_k(w) = \mathcal{N}(w; y_k, \sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(w-y_k)^2}{2\sigma^2}}$$

Variable prior

2. Check-to-variable : convolution of received messages (except recipient), periodize

$$g_{t,l}(w) = \sum_{i=-\infty}^{\infty} \mathcal{N}\left(w; m_{c,l} - \frac{i}{h_l}, \sigma^2_{c,l}\right)$$

~ compute marginal variable distribution

3. Variable-to-check : (variables treat incoming information as independent)

EXPENSIVE!

   a) Product of received messages (except recipient), and local message

   b) Normalization

   c) Approximation with single Gaussian

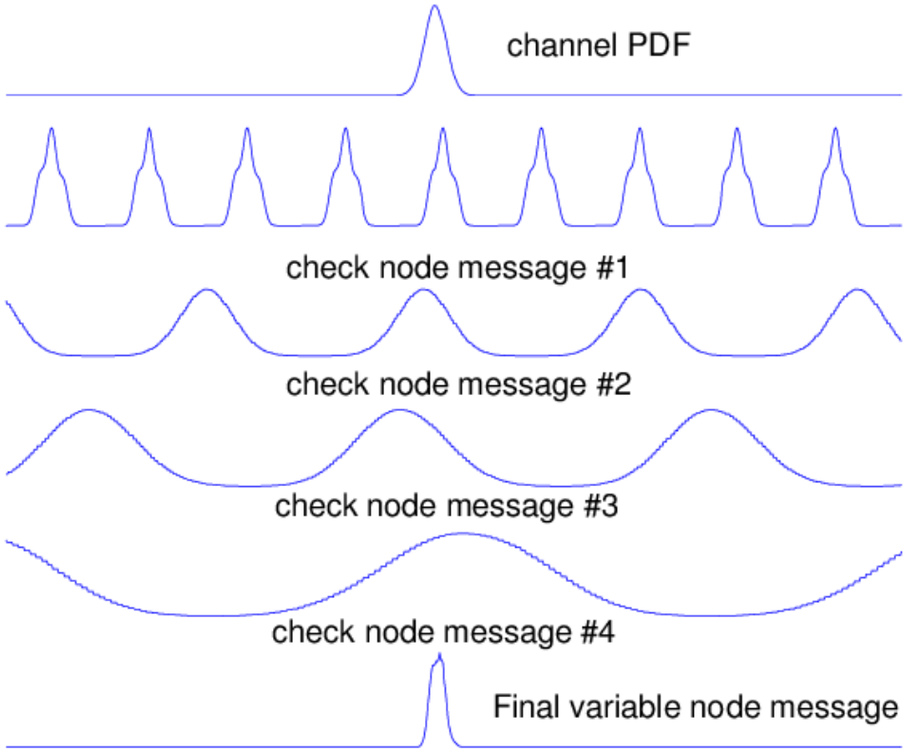
4. Decision : variables take product of messages, argmax, round

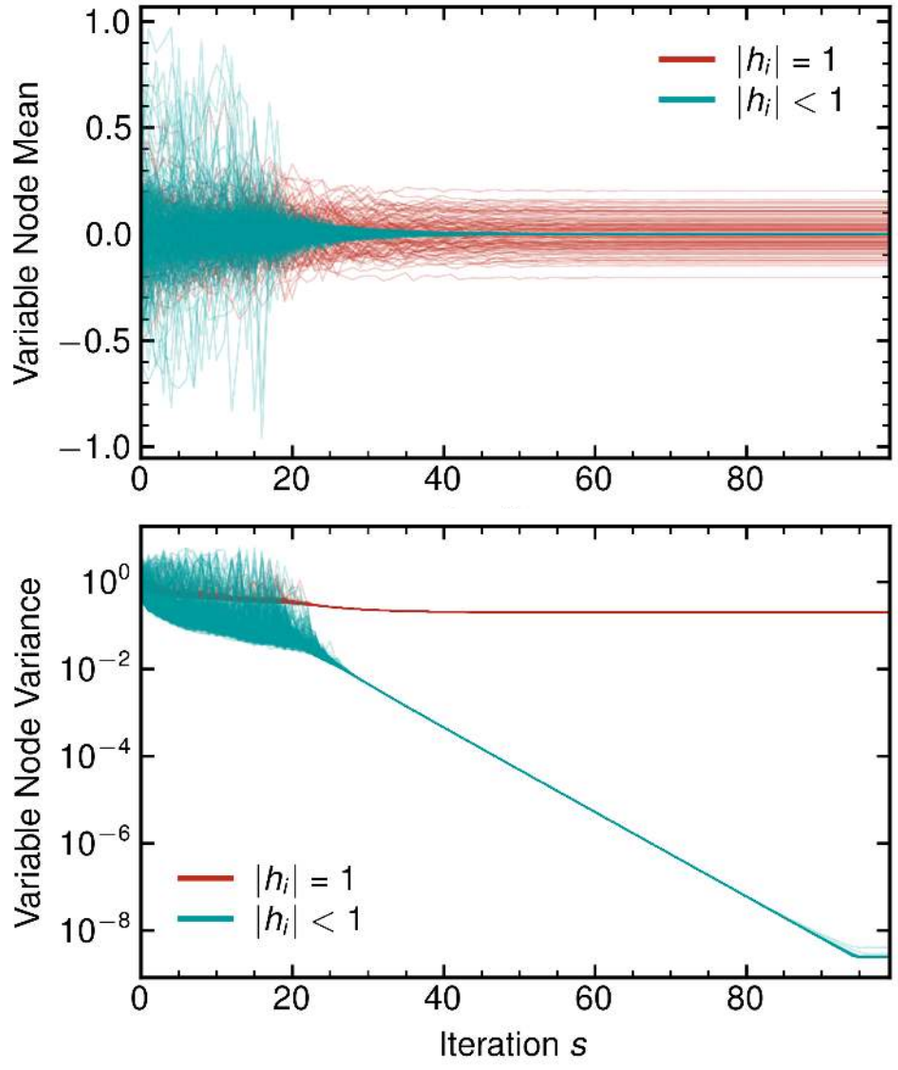
$$\hat{x}_k = \arg\max_w \hat{f}_k^{\text{final}}(w).$$

$$\hat{\mathbf{u}} = \lfloor \mathbf{H}\hat{\mathbf{x}} \rceil.$$

Classical results

Variances of ‘non-unit’ variable nodes converge to zero (exponentially fast!)

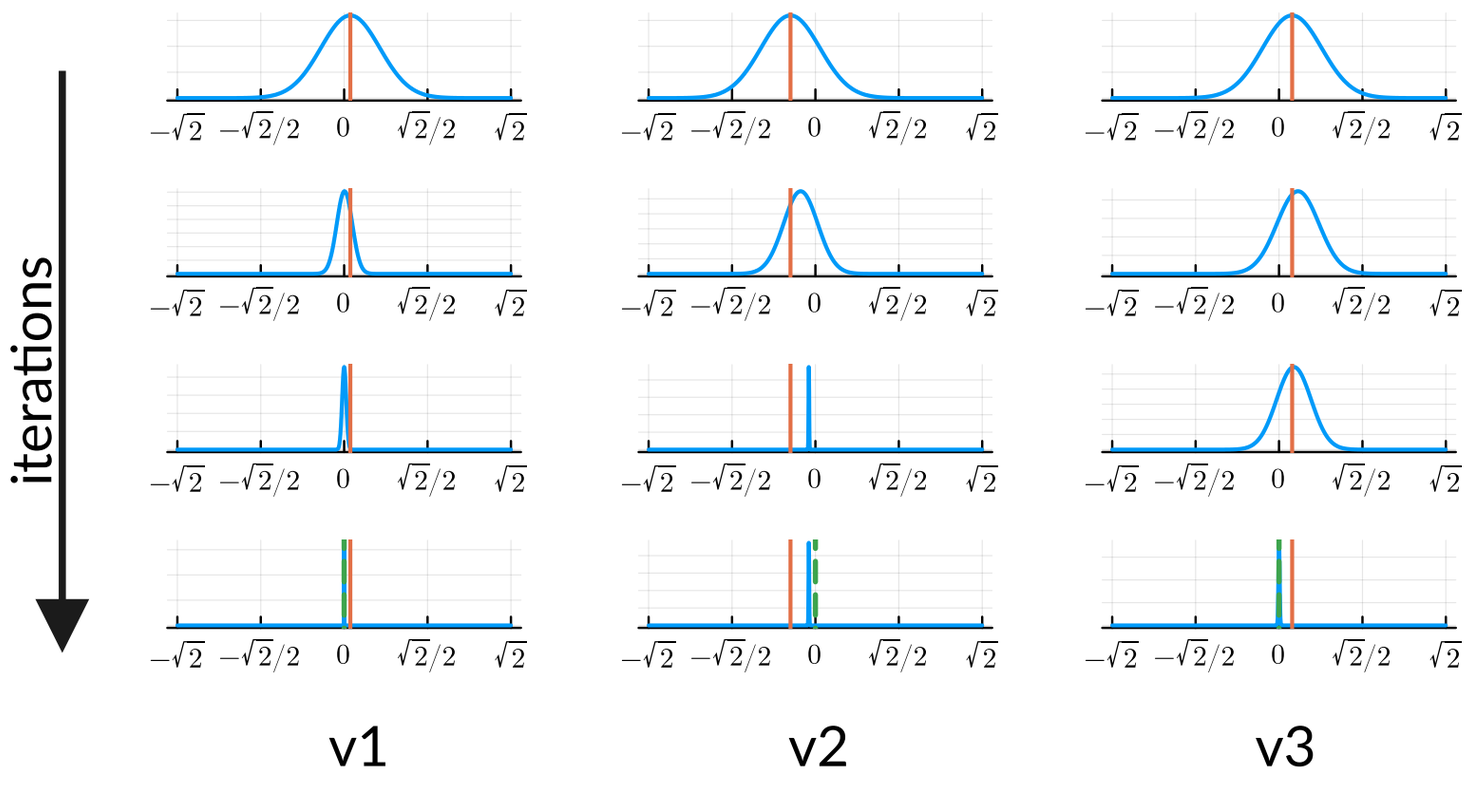


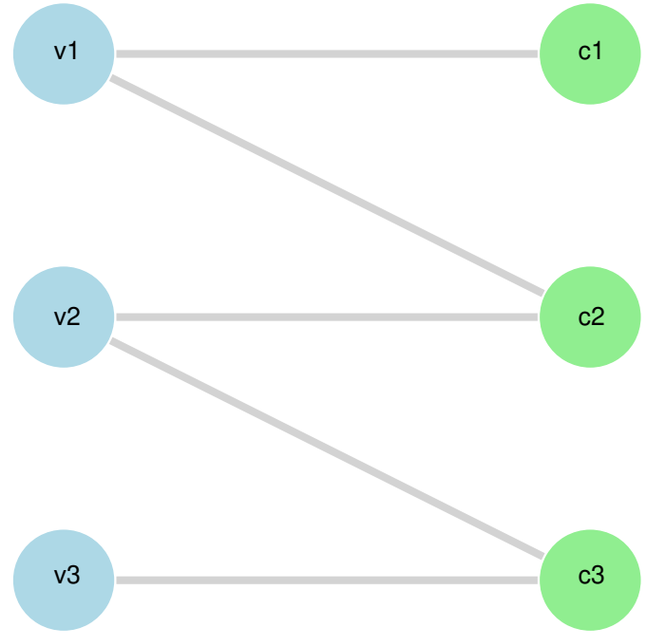


Visualizing BP

$$M = \frac{1}{\sqrt{2}} \left(\begin{array}{c|ccc} 2\mathbb{I} & & & \\ \hline & 2 & 0 & 0 \\ & 1 & 1 & 0 \\ & 0 & 1 & 1 \end{array} \right) \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \text{c1} \\ \text{c2} \\ \text{c3} \end{matrix}$$

$$\begin{matrix} \text{v1} & \text{v2} & \text{v3} \end{matrix}$$

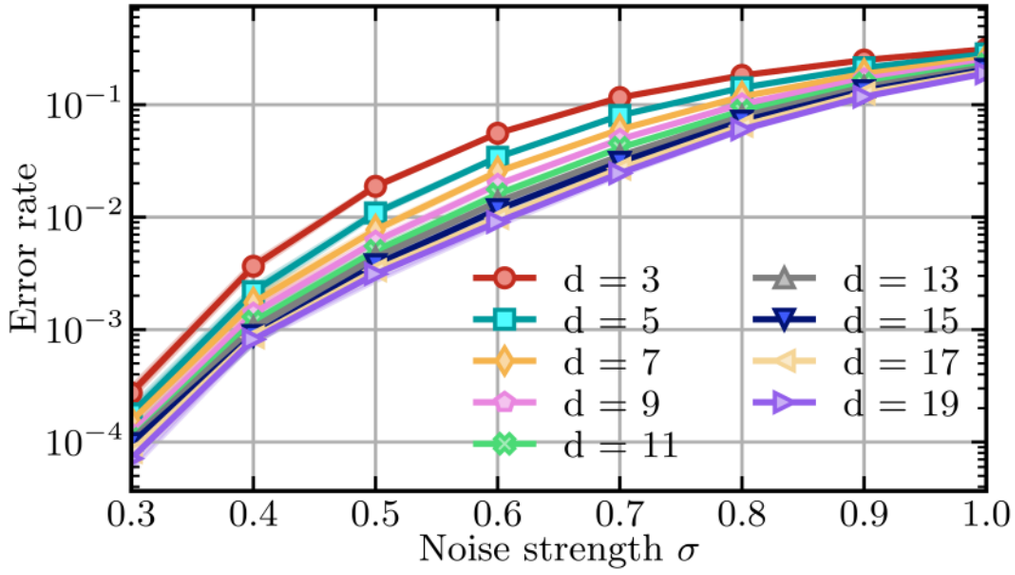


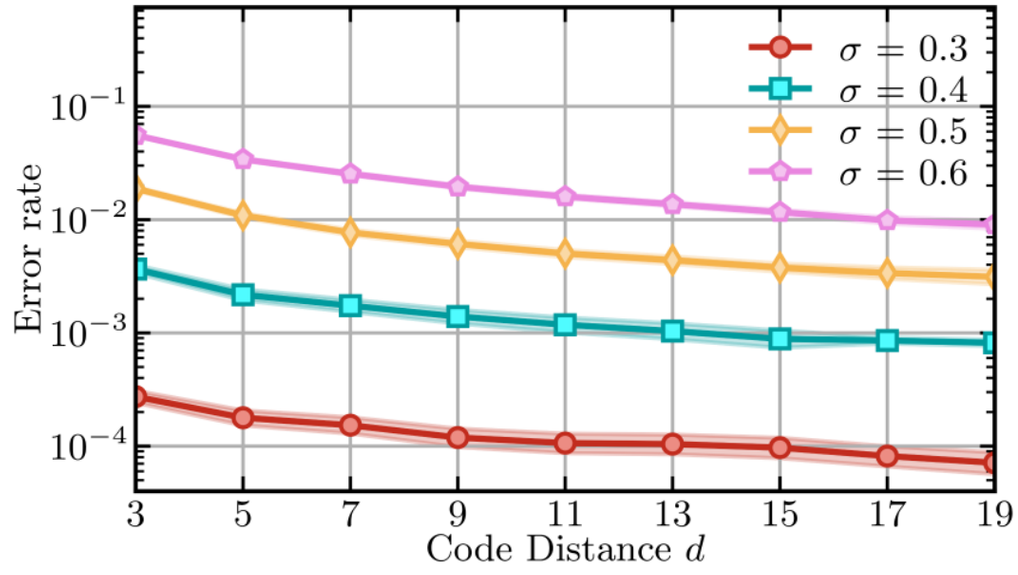


(decision is simulated at each iteration)

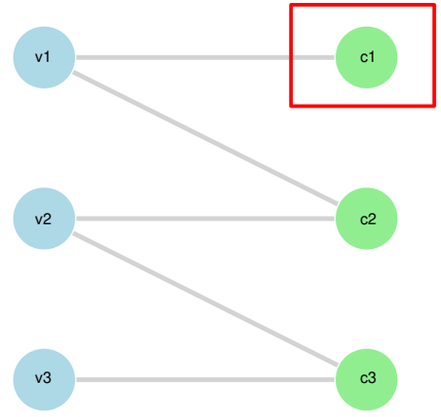
Decoding sparse concatenated codes?

Sort of works for GKP-repetition codes...BUT no exponential error suppression



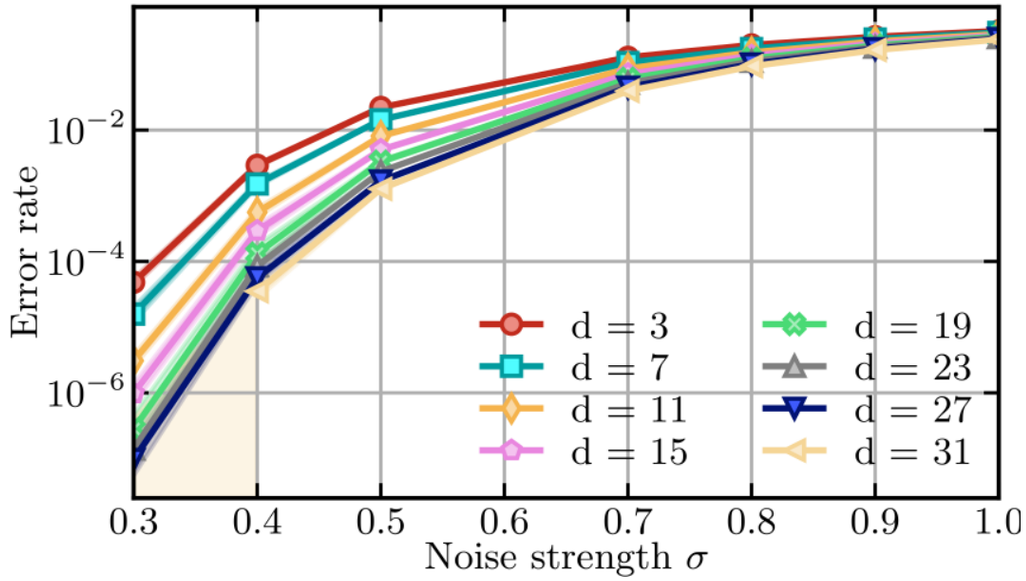


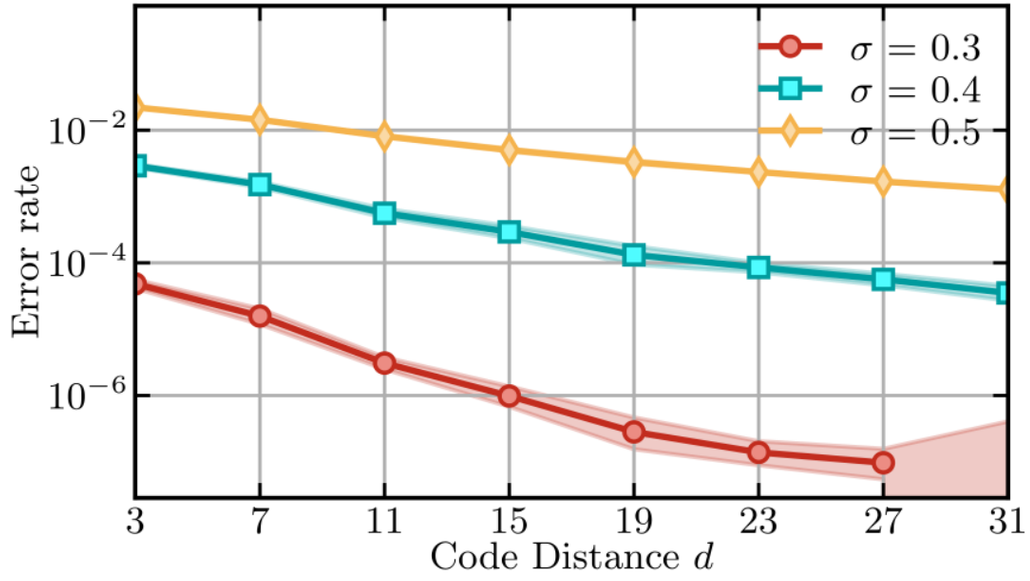
$$M = \frac{1}{\sqrt{2}} \left(\begin{array}{c|ccc} 2\mathbb{I} & & & \\ \hline & 2 & 0 & 0 \\ & 1 & 1 & 0 \\ & 0 & 1 & 1 \end{array} \right)$$



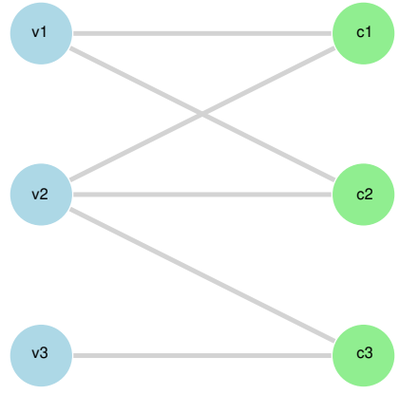
Decoding sparse concatenated codes?

Sort of works for GKP-repetition codes...BUT no exponential error suppression...
UNLESS we remove *dangling checks*



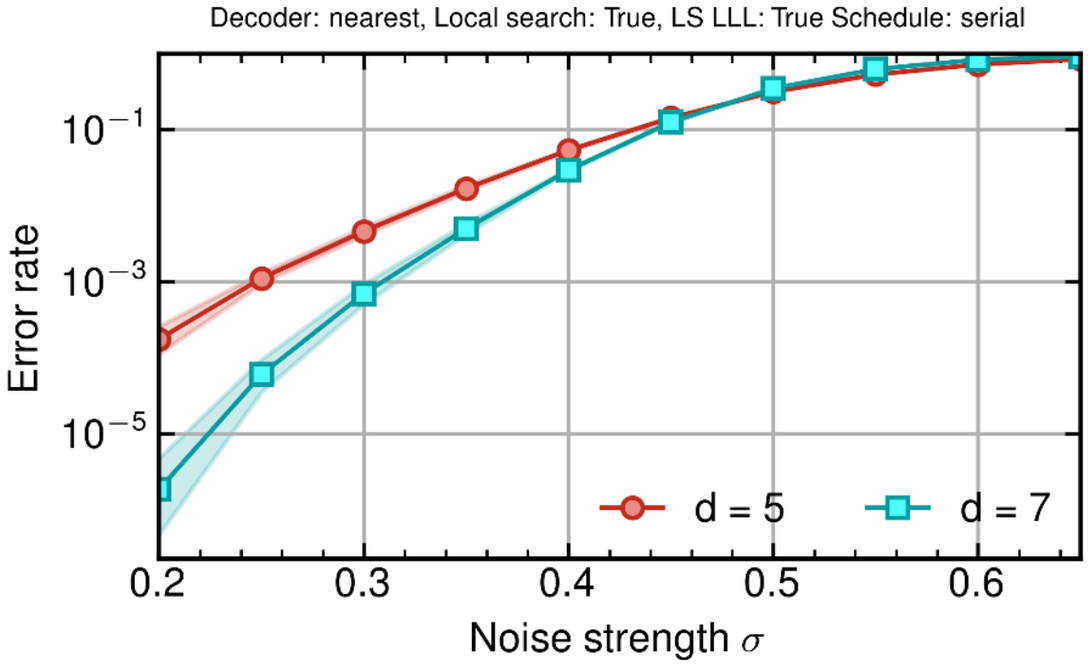


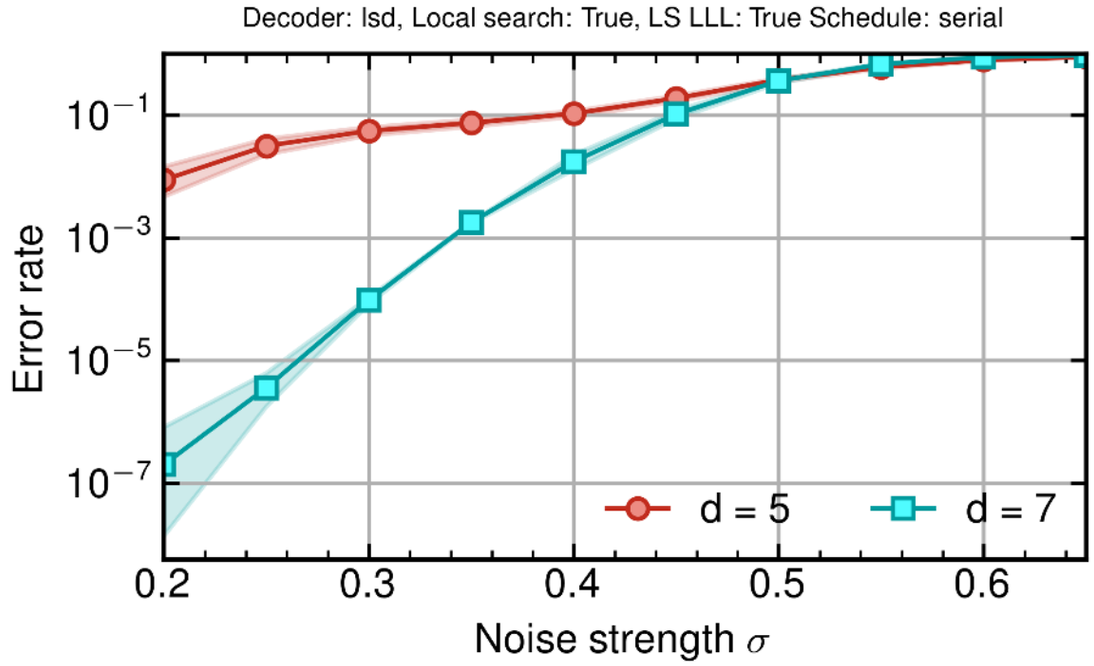
$$M = \frac{1}{\sqrt{2}} \left(\begin{array}{c|ccc} 2\mathbb{I} & & & \\ \hline & 1 & -1 & 0 \\ & 1 & 1 & 0 \\ & 0 & 1 & 1 \end{array} \right)$$



Decoding sparse concatenated codes?

How about true quantum codes? → small bivariate bicycle codes





Promising but hard to say:
too many hyperparameters →

- Variable update rule
- Update schedule
- ‘’Local search’’ (~OSD)
- Message update schedule
- …

Bosonic low-density lattice codes? (trivial)

Each row/column: exactly d non-zero entries, typically

Sommer, Feder, Shalvi, IEEE TIT 54 (2008)

$$h_1 = \pm 1, \quad h_2, \ldots, h_d = \pm \frac{1}{\sqrt{d}}$$

(magic square LDLC)

Random construction, no length-4 cycles

If $\sqrt{d} \in \mathbb{Z} \Rightarrow \sqrt{d}H$ has integer entries $\Rightarrow dHJH^T$ has integer entries

logical dimension becomes very large ⇨ code parameters are almost always terrible

Can we do better?

Bosonic low-density lattice codes: reduce dimension

$$M = \begin{pmatrix} M_q & 0 \\ 0 & M_p \end{pmatrix} = \begin{pmatrix} c_q H_1 & 0 \\ 0 & c_p H_2 \end{pmatrix}$$

Canonical lattice basis:

$$M_{\mathrm{can}} J M_{\mathrm{can}}^T = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \qquad D = \mathrm{diag}\left(d_1, \ldots, d_n\right), \quad d \in \mathbb{N}^+$$

Bosonic low-density lattice codes: reduce dimension

$$M = \begin{pmatrix} M_q & 0 \\ 0 & M_p \end{pmatrix} = \begin{pmatrix} c_q H_1 & 0 \\ 0 & c_p H_2 \end{pmatrix}$$

Canonical lattice basis:

$$M_{\mathrm{can}} J M_{\mathrm{can}}^T = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \qquad D = \mathrm{diag}\left(d_1, \ldots, d_n\right), \quad d \in \mathbb{N}^+$$

$$D_{jj} = M_{\mathrm{can}}(j, \cdot) J M_{\mathrm{can}}(j+n, \cdot)$$

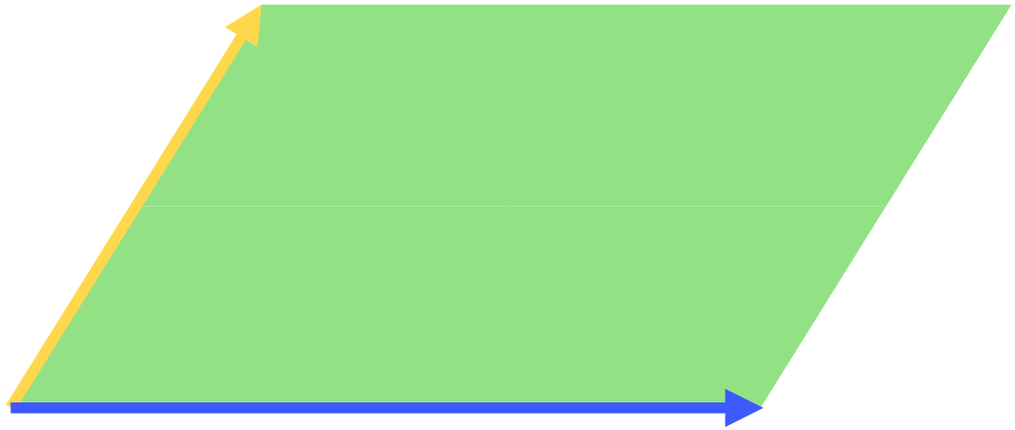
Bosonic low-density lattice codes: reduce dimension

$$M = \begin{pmatrix} M_q & 0 \\ 0 & M_p \end{pmatrix} = \begin{pmatrix} c_q H_1 & 0 \\ 0 & c_p H_2 \end{pmatrix}$$

Canonical lattice basis:

$$M_{\mathrm{can}} J M_{\mathrm{can}}^T = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \qquad D = \mathrm{diag}\left(d_1, \ldots, d_n\right), \quad d \in \mathbb{N}^+$$

$$D_{jj} = 2$$



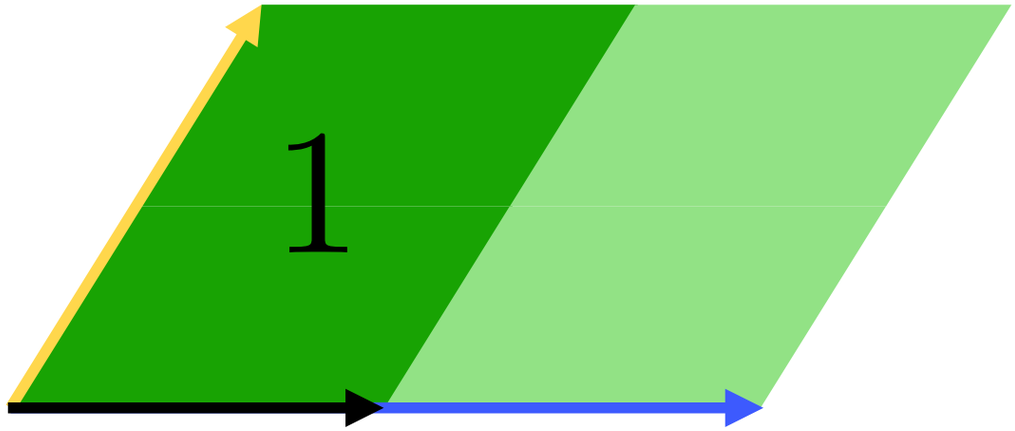
Bosonic low-density lattice codes: reduce dimension

$$M = \begin{pmatrix} M_q & 0 \\ 0 & M_p \end{pmatrix} = \begin{pmatrix} c_q H_1 & 0 \\ 0 & c_p H_2 \end{pmatrix}$$

Canonical lattice basis:

$$M_{\mathrm{can}} J M_{\mathrm{can}}^T = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \qquad D = \mathrm{diag}\left(d_1, \ldots, d_n\right), \quad d \in \mathbb{N}^+$$

$$D_{jj} = 2$$



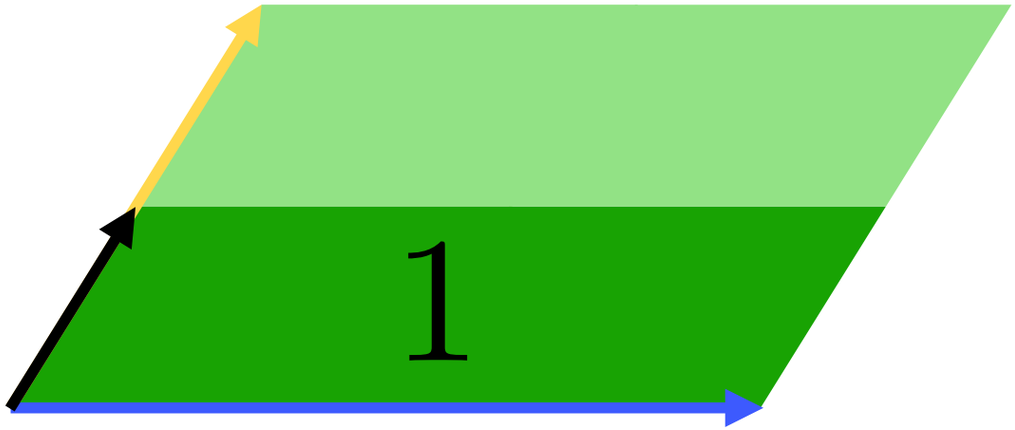
Bosonic low-density lattice codes: reduce dimension

$$M = \begin{pmatrix} M_q & 0 \\ 0 & M_p \end{pmatrix} = \begin{pmatrix} c_q H_1 & 0 \\ 0 & c_p H_2 \end{pmatrix}$$

Canonical lattice basis:

$$M_{\mathrm{can}} J M_{\mathrm{can}}^T = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \qquad D = \mathrm{diag}\left(d_1, \ldots, d_n\right), \quad d \in \mathbb{N}^+$$

$$D_{jj} = 2$$



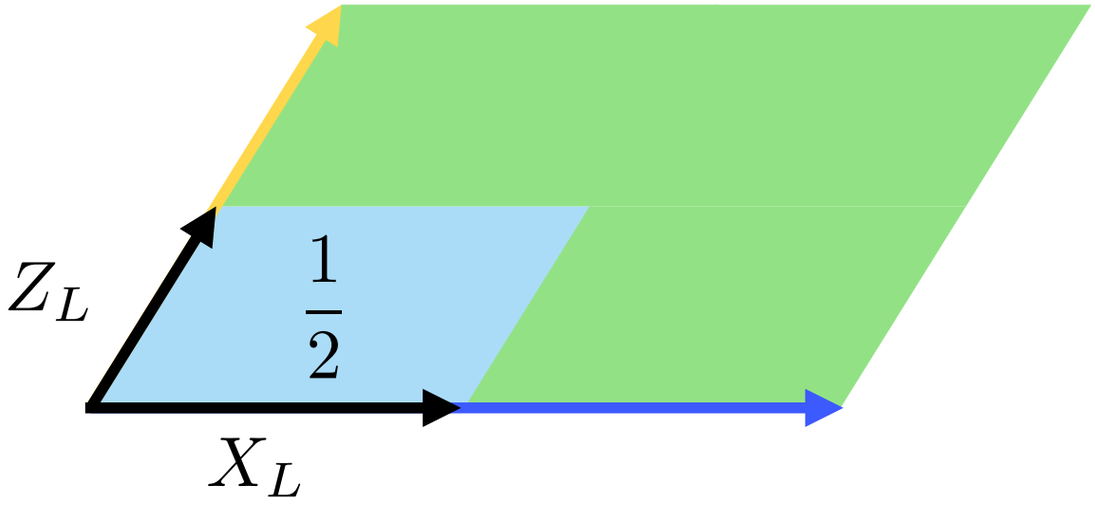
Bosonic low-density lattice codes: reduce dimension

$$M = \begin{pmatrix} M_q & 0 \\ 0 & M_p \end{pmatrix} = \begin{pmatrix} c_q H_1 & 0 \\ 0 & c_p H_2 \end{pmatrix}$$

Canonical lattice basis:

$$M_{\mathrm{can}} J M_{\mathrm{can}}^T = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \qquad D = \mathrm{diag}\left(d_1, \ldots, d_n\right), \quad d \in \mathbb{N}^+$$

$$D_{jj} = 2$$



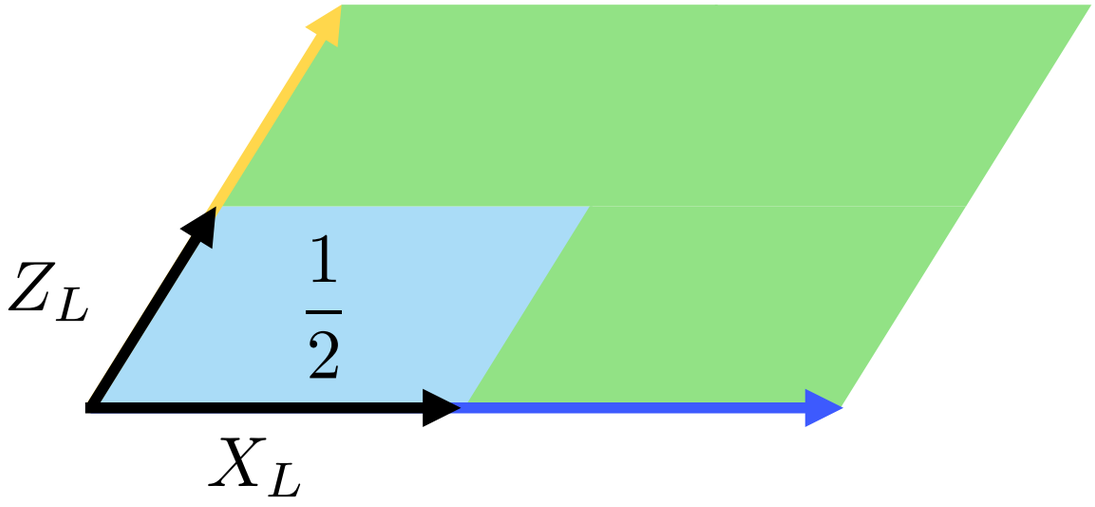
Bosonic low-density lattice codes: reduce dimension

$$M = \begin{pmatrix} M_q & 0 \\ 0 & M_p \end{pmatrix} = \begin{pmatrix} c_q H_1 & 0 \\ 0 & c_p H_2 \end{pmatrix}$$

Canonical lattice basis:

$$M_{\mathrm{can}} J M_{\mathrm{can}}^T = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \qquad D = \mathrm{diag}\left(d_1, \ldots, d_n\right), \quad d \in \mathbb{N}^+$$

$$D_{jj} = 2$$



Non unique:
different qudit decompositions

Burchards, Flammia, Conrad, Quantum (2025)

Frobenius standard form (unique)

$$D_{jj} \,|\, D_{j-1,j-1}$$

Can be computed efficiently!

Kuperberg, Kasteleyn Cokernels. Electr. J. Comb. 9(1), 2002

Bosonic low-density lattice codes: reduce dimension

1. Create random classical LDLC and define $M = cH; \quad MJM^T \in \mathbb{Z}^{2n\times 2n}$

2. Find canonical basis in Frobenius SF

If not, restart

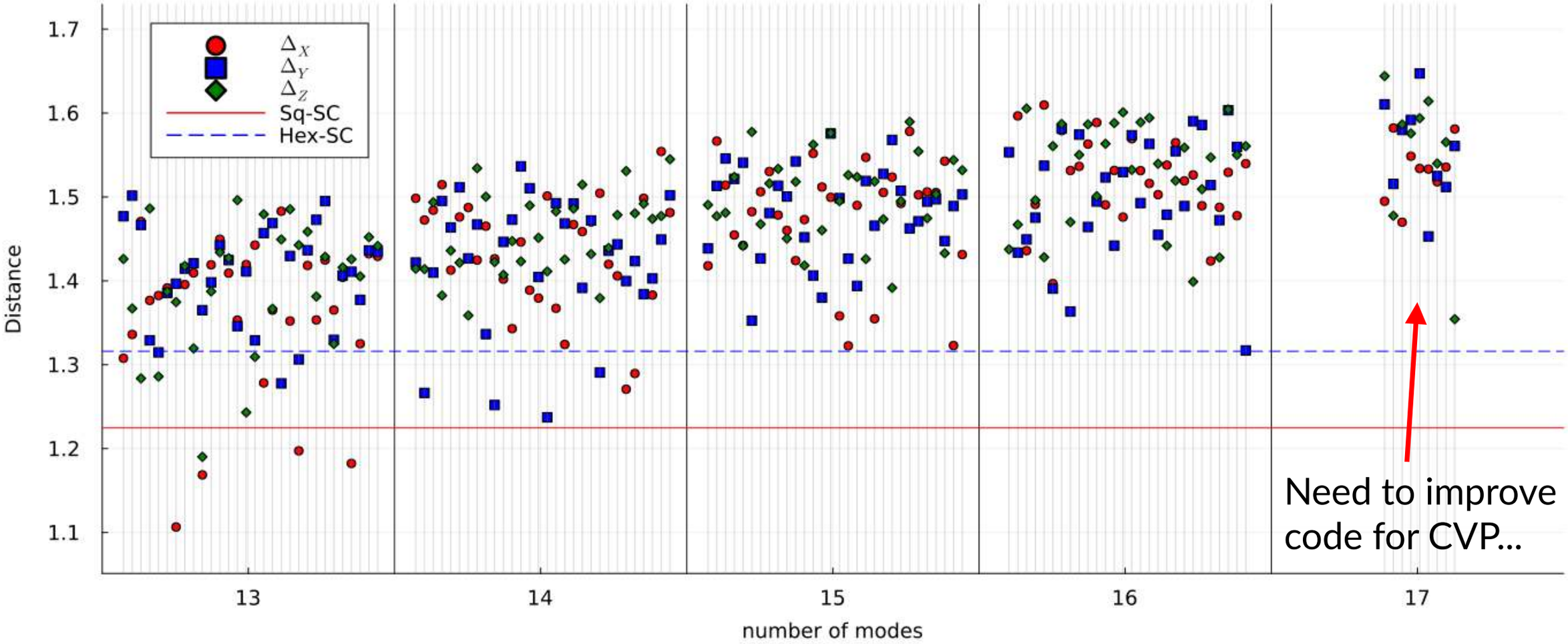
$$M_{\mathrm{F}} J M_{\mathrm{F}}^T = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \qquad D = \mathrm{diag}\left(1, 1, \ldots, 1, \boxed{2z_1 z_2}\right), \quad z_1, z_2 \in \mathbb{N}^+$$

3. Add $\boldsymbol{u} = \dfrac{M_{\mathrm{F}}(n,\cdot)}{z_1}; \quad \boldsymbol{v} = \dfrac{M_{\mathrm{F}}(2n,\cdot)}{z_2}$ as rows to M, reduce → $\boxed{\begin{array}{c} M_Q \\ \text{Logical qubit} \end{array}}$

4. Define: $\mathrm{X}_L = D\left(\frac{\boldsymbol{u}}{2}\right); \quad Z_L = D\left(\frac{\boldsymbol{v}}{2}\right)$

5. Find short representatives, e.g. : $\mathrm{X}_L \mapsto D\left(\frac{\tilde{\boldsymbol{u}}}{2}\right); \quad \tilde{u} = \mathrm{argmin}_{\boldsymbol{z}\in\mathbb{Z}^{2n}} \left|\left|\frac{\boldsymbol{u}}{2} - M_Q^T \boldsymbol{z}\right|\right|$

Dimension-reduced qLDLCs: distance



Small instances have **larger distances than surface codes** on the same modes!

Drawback: M_Q is almost sparse (two dense rows) → Unclear if BP will work... TODO

Conclusions

- Many promising results, few certainties
- Concatenation from multi-mode might have good balance parameters/complexity
- There is potentially much we can adapt from classical lattice codes but...
- Can we make Gaussian BP work consistently?

Positions available!

https://qat.inria.fr/

Thank you!