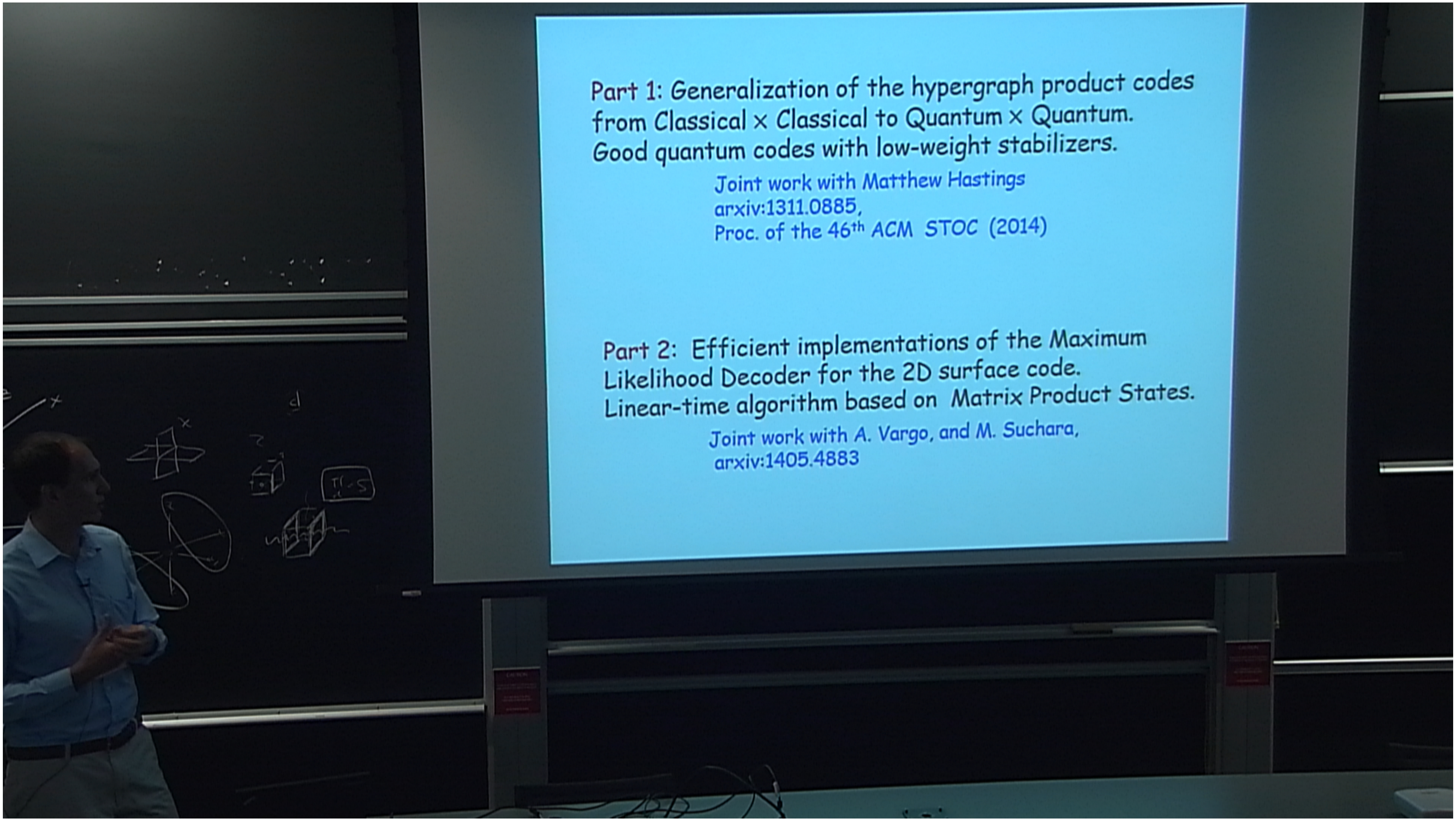
Title: Homological product codes

Date: Jul 16, 2014 10:30 AM

URL: http://pirsa.org/14070013

Abstract: <span>All examples of quantum LDPC codes known to this date suffer from a poor distance scaling limited by the square-root of the code length. This is in a sharp contrast with the classical case where good LDPC codes are known that combine constant encoding rate and linear distance. In this talk I will describe the first family of good quantum "almost LDPC" codes. The new codes have a constant encoding rate, linear distance, and stabilizers acting on at most square root of n qubits, where n is the code length. For comparison, all previously known families of good quantum codes have stabilizers of linear weight. The proof combines two techniques: randomized constructions of good quantum codes and the homological product operation from algebraic topology. We conjecture that similar methods can produce good quantum codes with stabilizer weight n^a for any a>0. Finally, we apply the homological product to construct new small codes with low-weight stabilizers.<br><br>This is a joint work with Matthew Hastings<br>Preprint: arXiv:1311.0885</span>


Part 1: Generalization of the hypergraph product codes
from Classical × Classical to Quantum × Quantum.
Good quantum codes with low-weight stabilizers.
Joint work with Matthew Hastings
arxiv:1311.0885,
Proc. of the 46th ACM STOC (2014)
Part 2: Efficient implementations of the Maximum
Likelihood Decoder for the 2D surface code.
Linear-time algorithm based on Matrix Product States.
Joint work with A. Vargo, and M. Suchara,
arxiv:1405.4883

# How good can be quantum LDPC codes ?

| | k | d | w |
|---|---|---|---|
| 2D Surface Codes (SC) [1] | $O(1)$ | $n^{1/2}$ | 4 |
| 2D Hyperbolic SC [2] | $\Omega(n)$ | $\log(n)$ | $O(1)$ |
| 3D Generalized SC [3] | $O(1)$ | $(n \log n)^{1/2}$ | $O(1)$ |
| Hypergraph Product Codes [4] (almost good) | $\Omega(n)$ | $n^{1/2}$ | $O(1)$ |

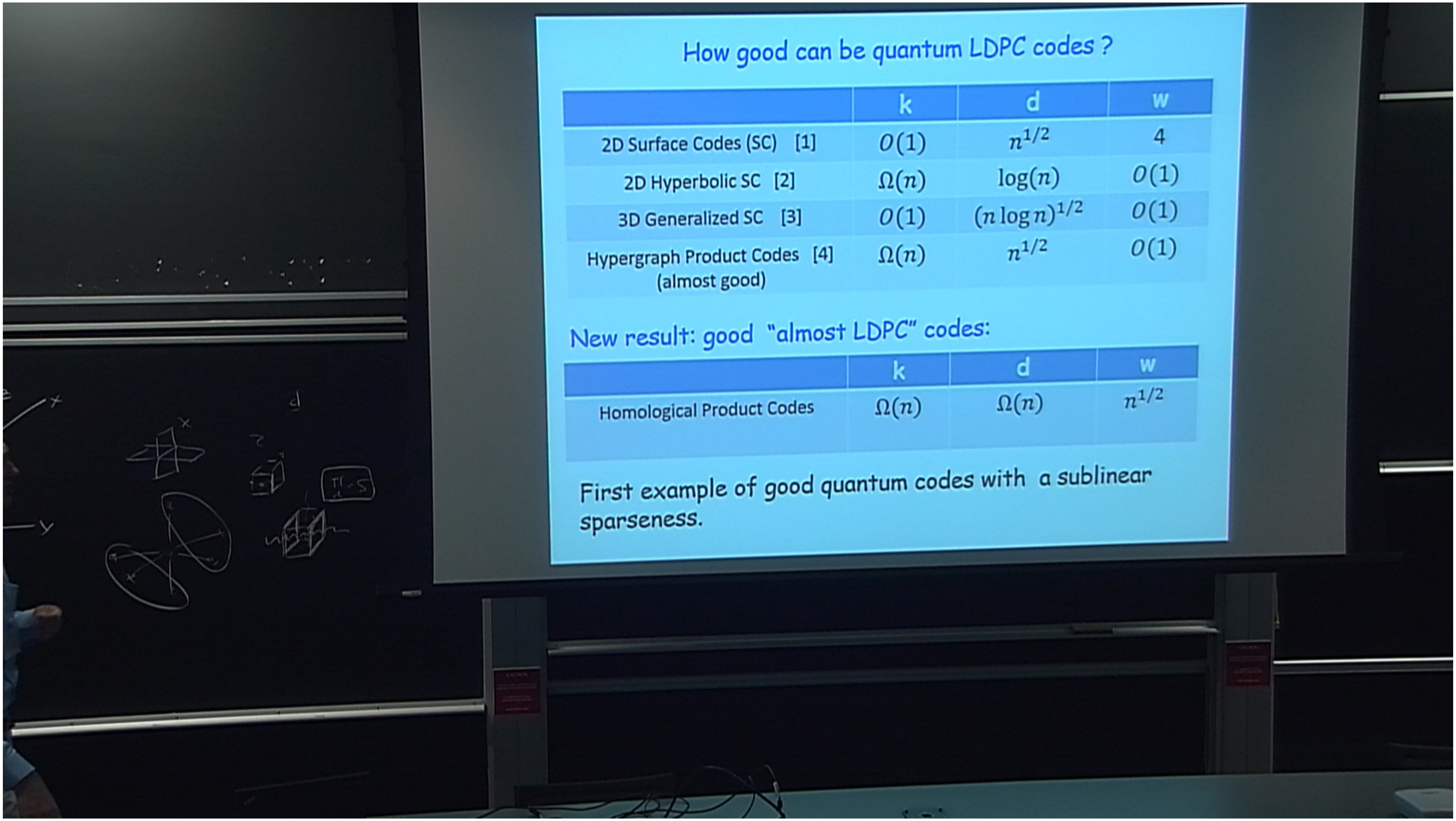
k = number of logical qubits
d = code distance
w = sparseness

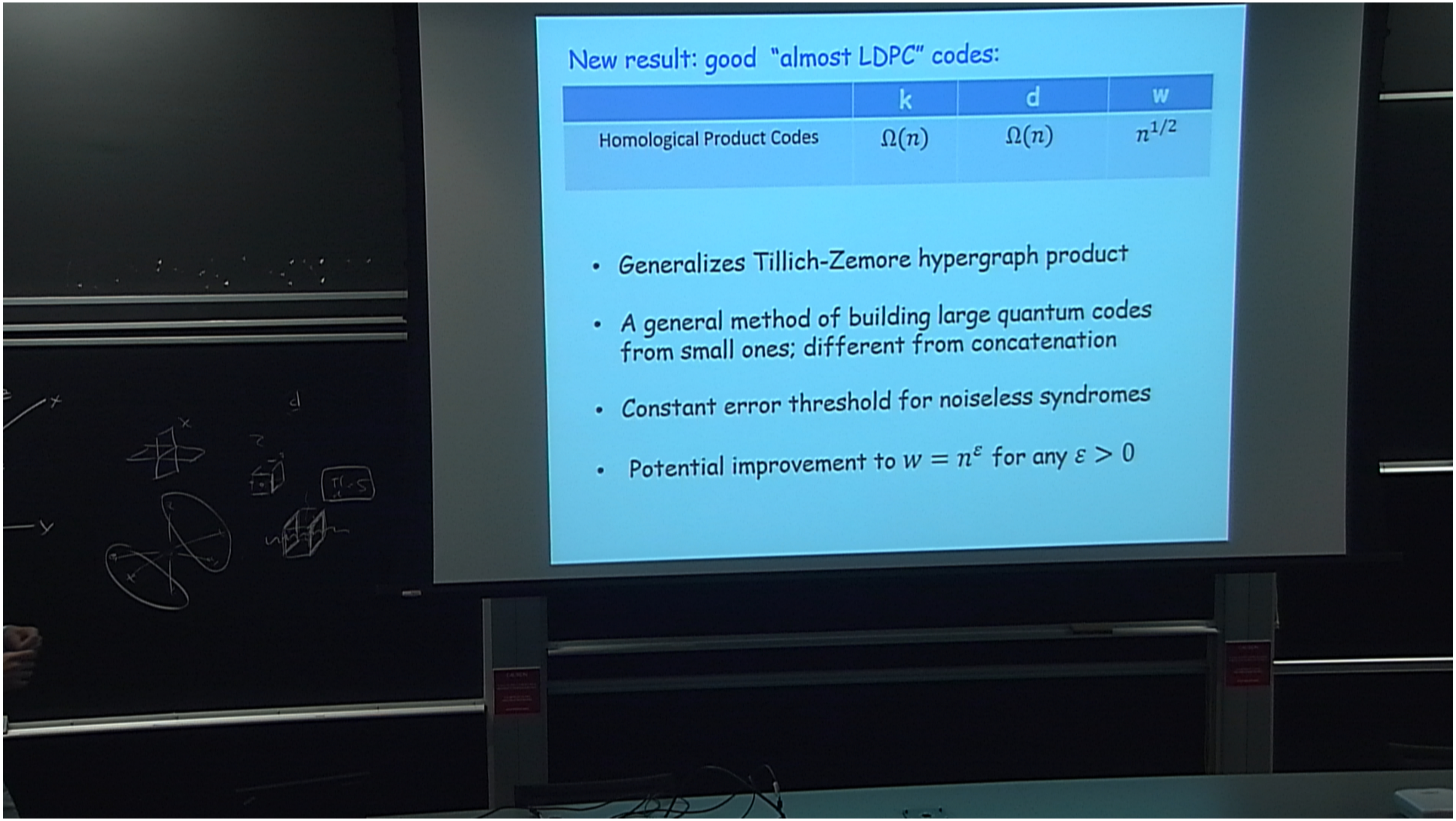

[1] Kitaev (1997)
[2] Zemor (2009); Delfosse (2013)
[3] Freedman, Meyer, Luo (2002)
[4] Tillich, Zemor (2009); Kovalev, Pryadko (2012); Freedman, Hastings (2013)

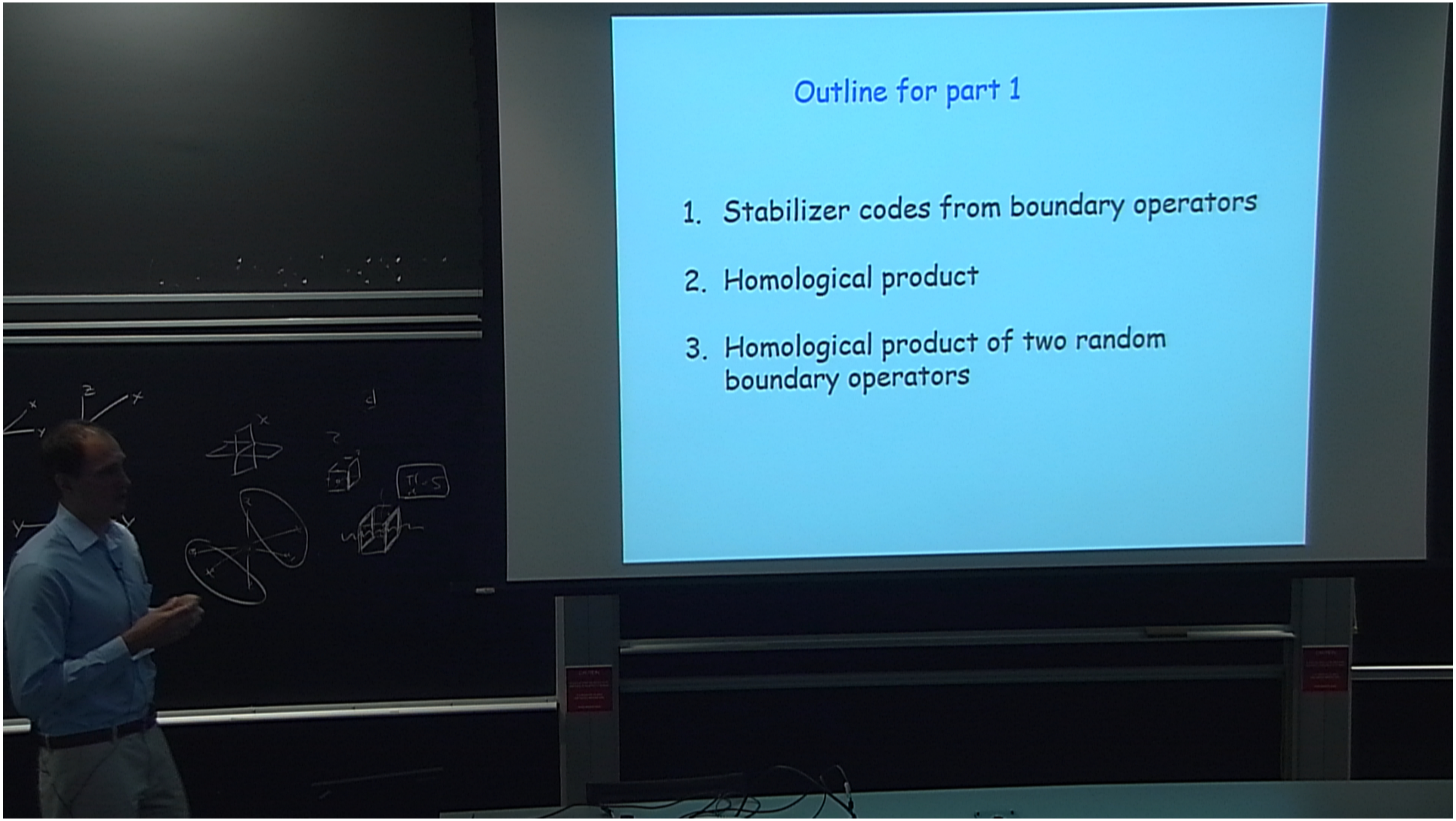
# How good can be quantum LDPC codes ?

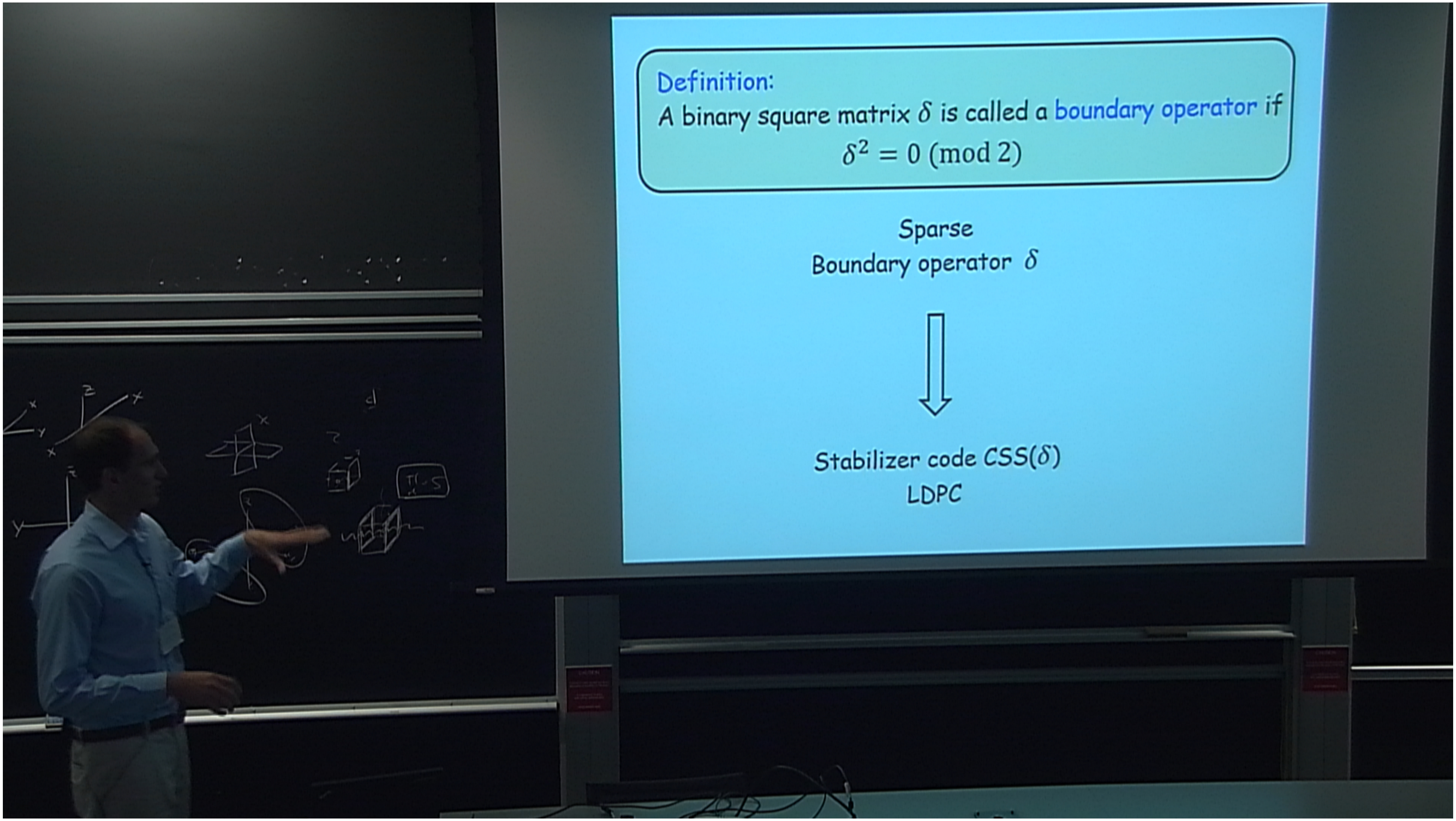
| | k | d | w |
|---|---|---|---|
| 2D Surface Codes (SC) [1] | $O(1)$ | $n^{1/2}$ | 4 |
| 2D Hyperbolic SC [2] | $\Omega(n)$ | $\log(n)$ | $O(1)$ |
| 3D Generalized SC [3] | $O(1)$ | $(n \log n)^{1/2}$ | $O(1)$ |
| Hypergraph Product Codes [4] (almost good) | $\Omega(n)$ | $n^{1/2}$ | $O(1)$ |

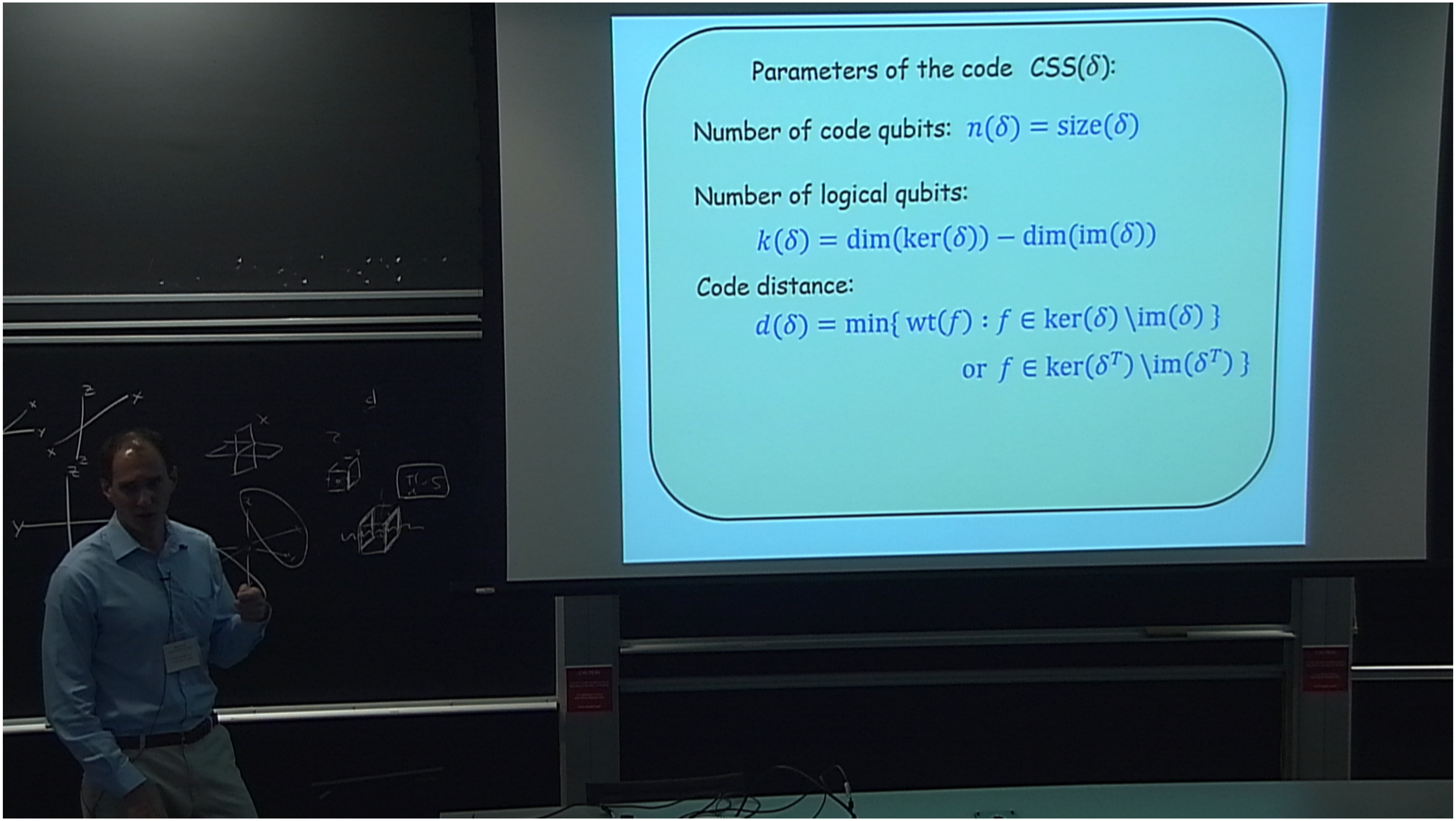
Open problem : find good quantum LDPC codes ($k$ and $d$ are linear in $n$) or prove that such codes do not exist.

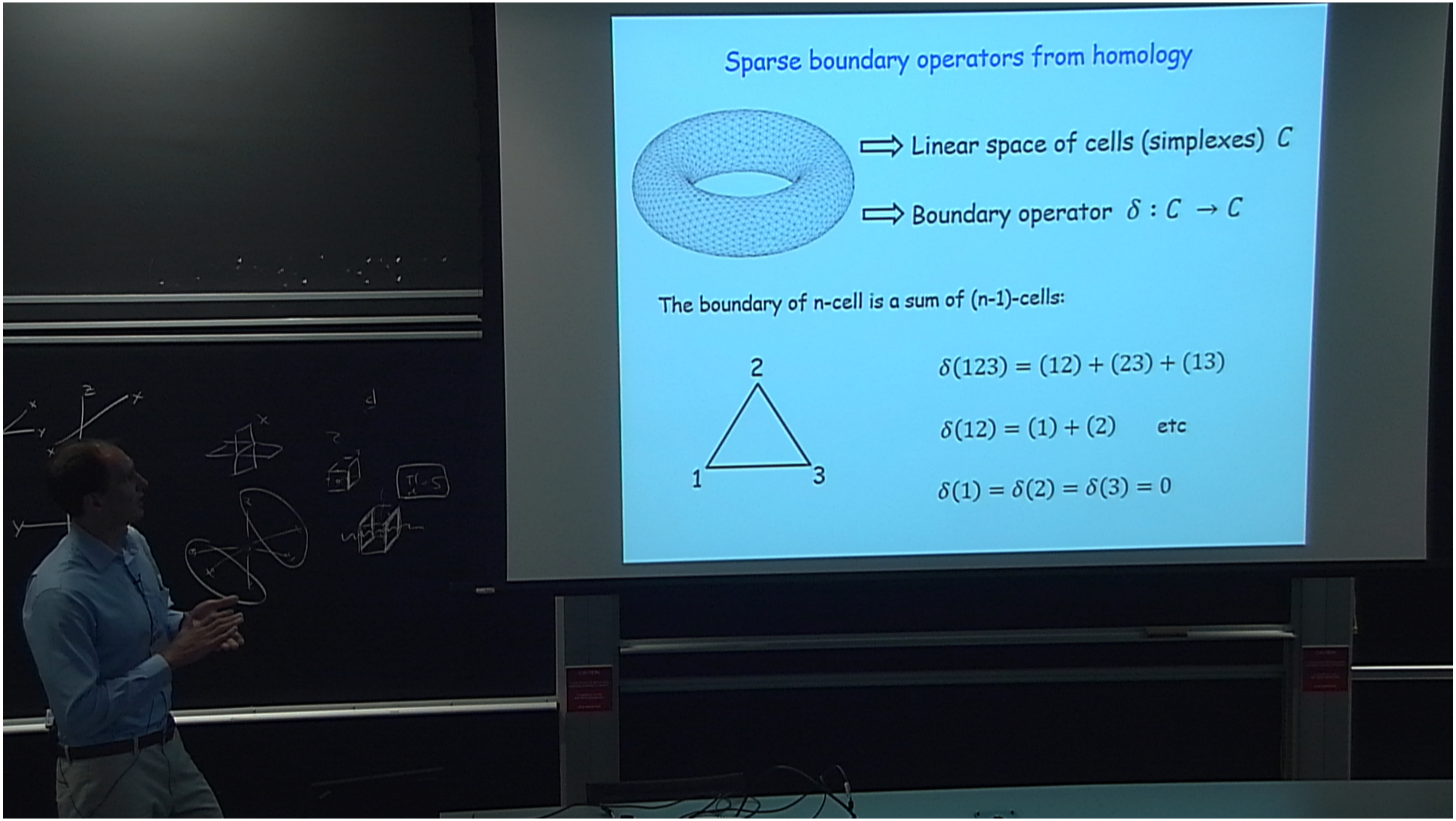

How good can be quantum LDPC codes ?
k
d
w
2D Surface Codes (SC) [1]
$O(1)$
$n^{1/2}$
4
2D Hyperbolic SC [2]
$\Omega(n)$
$\log(n)$
$O(1)$
3D Generalized SC [3]
$O(1)$
$(n \log n)^{1/2}$
$O(1)$
Hypergraph Product Codes [4]
(almost good)
$\Omega(n)$
$n^{1/2}$
$O(1)$
New result: good "almost LDPC" codes:
k
d
w
Homological Product Codes
$\Omega(n)$
$\Omega(n)$
$n^{1/2}$
First example of good quantum codes with a sublinear sparseness.

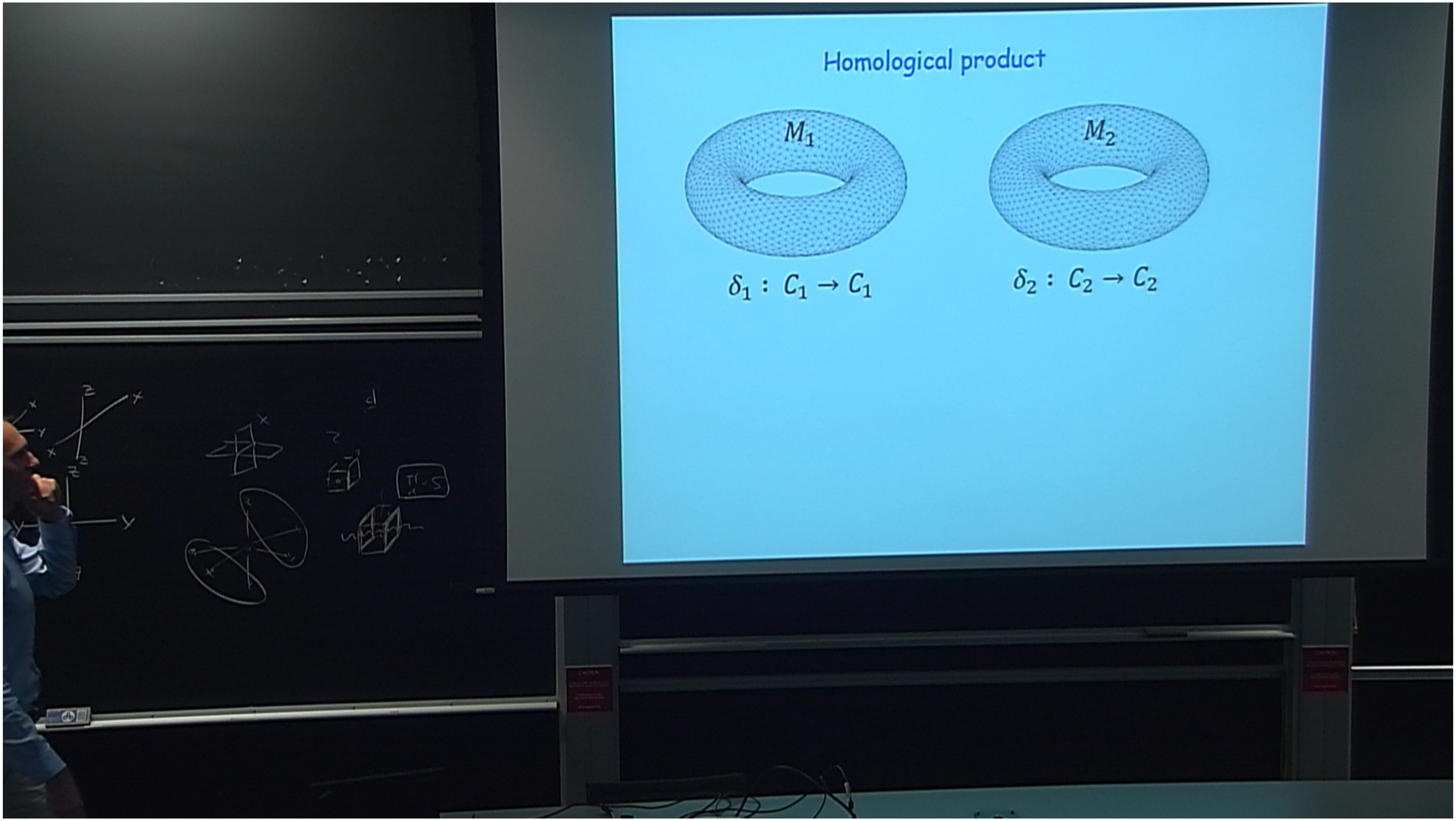

New result: good "almost LDPC" codes:
k
d
w
Homological Product Codes
$\Omega(n)$
$\Omega(n)$
$n^{1/2}$
Generalizes Tillich-Zemore hypergraph product
A general method of building large quantum codes from small ones; different from concatenation
Constant error threshold for noiseless syndromes
Potential improvement to $w = n^{\varepsilon}$ for any $\varepsilon > 0$

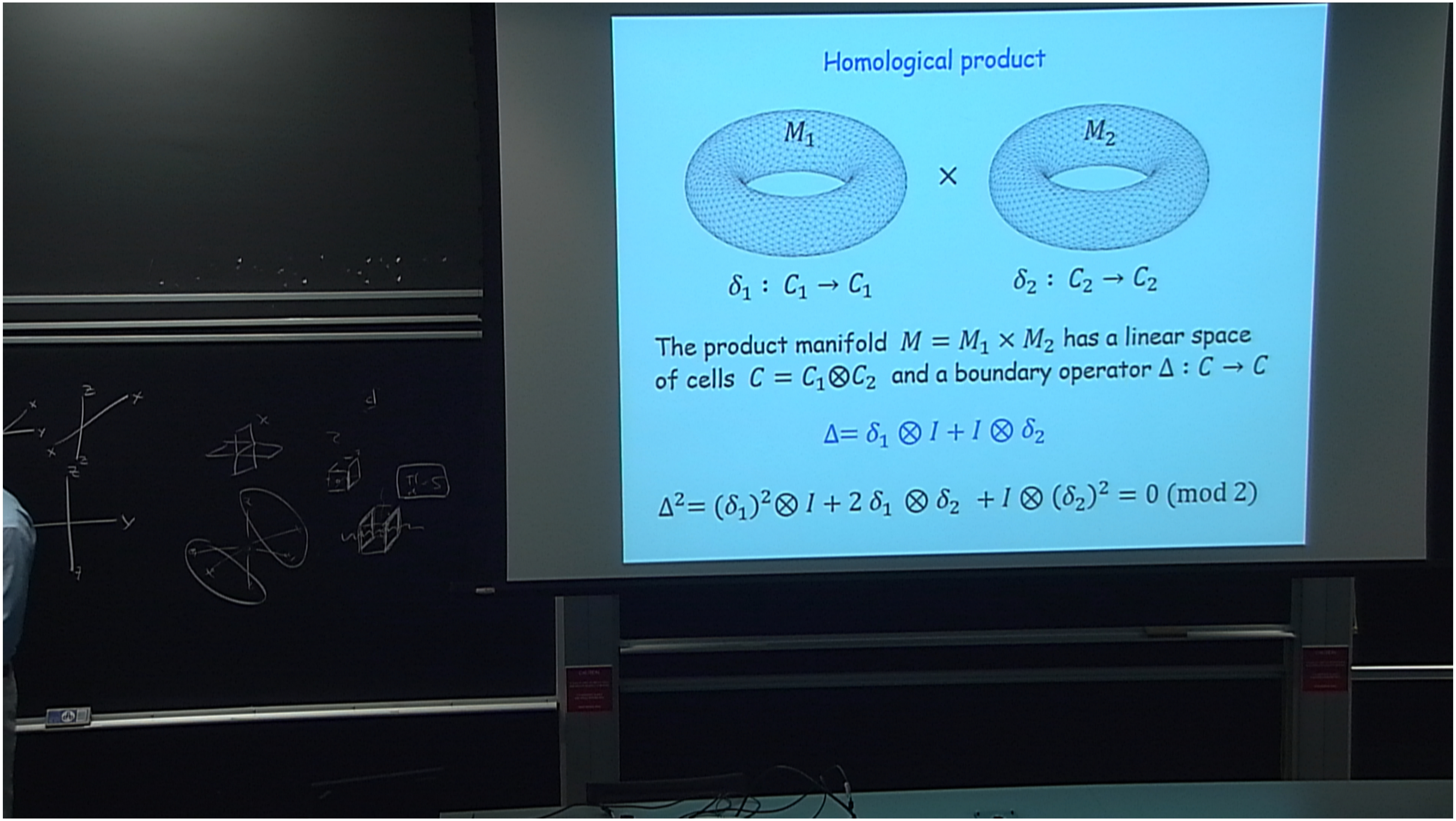

Outline for part 1
1. Stabilizer codes from boundary operators
2. Homological product
3. Homological product of two random boundary operators

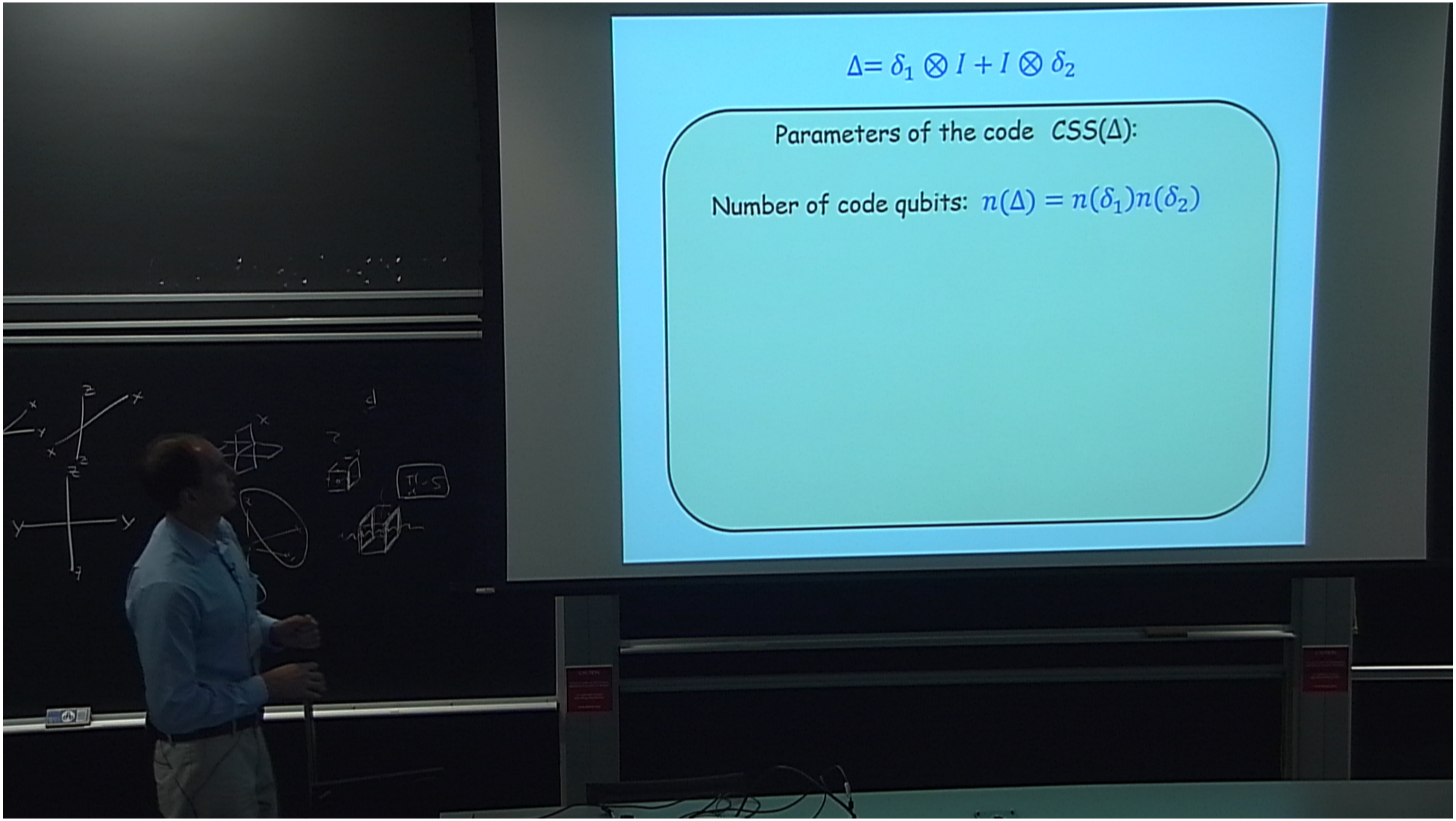

Definition:
A binary square matrix $\delta$ is called a boundary operator if
$\delta^2 = 0 \pmod 2$
Sparse
Boundary operator $\delta$
Stabilizer code CSS($\delta$)
LDPC

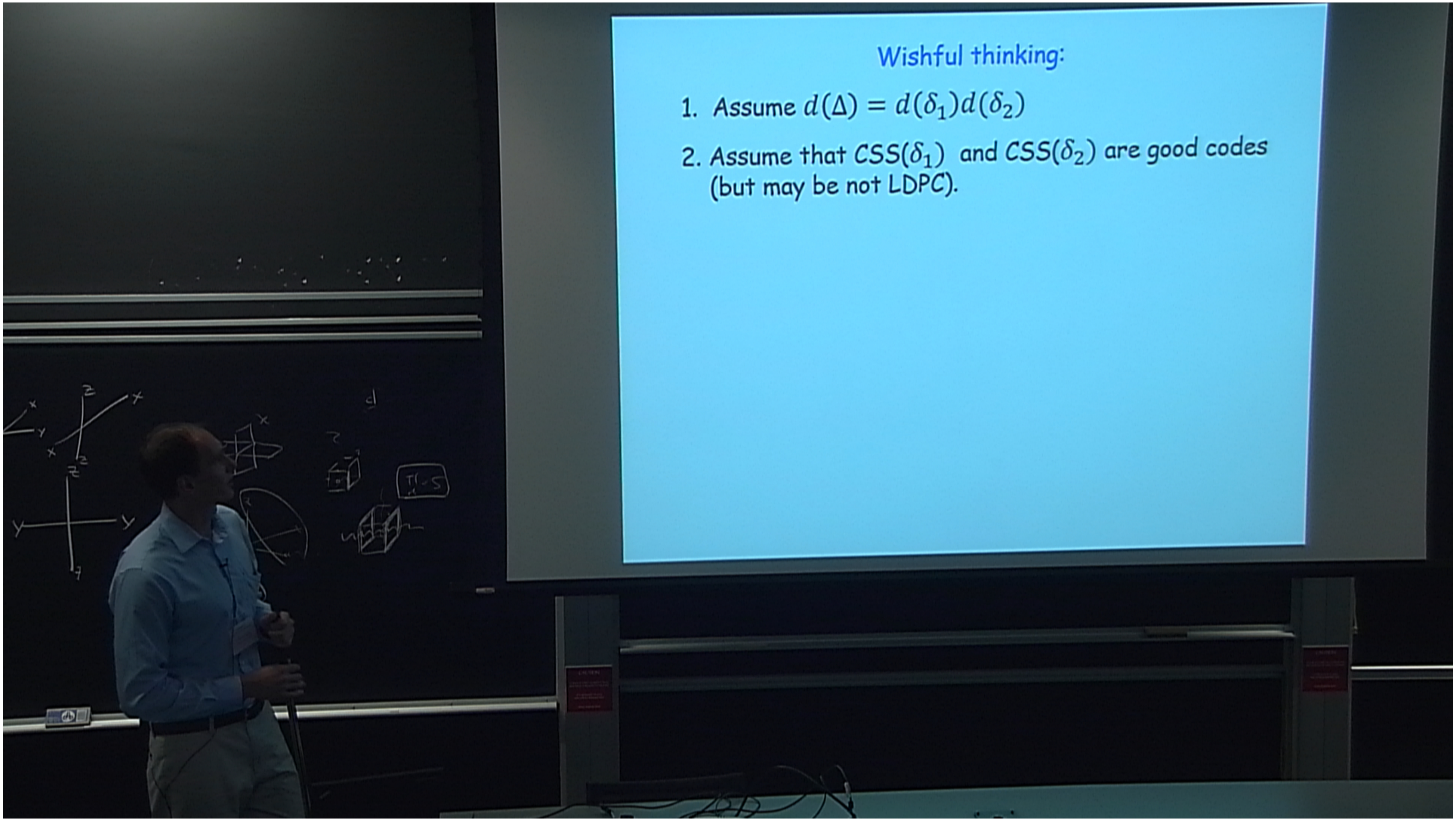

Parameters of the code CSS(δ):
Number of code qubits: n(δ) = size(δ)
Number of logical qubits:
k(δ) = dim(ker(δ)) − dim(im(δ))
Code distance:
d(δ) = min{ wt(f) : f ∈ ker(δ) \im(δ) }
or f ∈ ker(δ^T) \im(δ^T) }

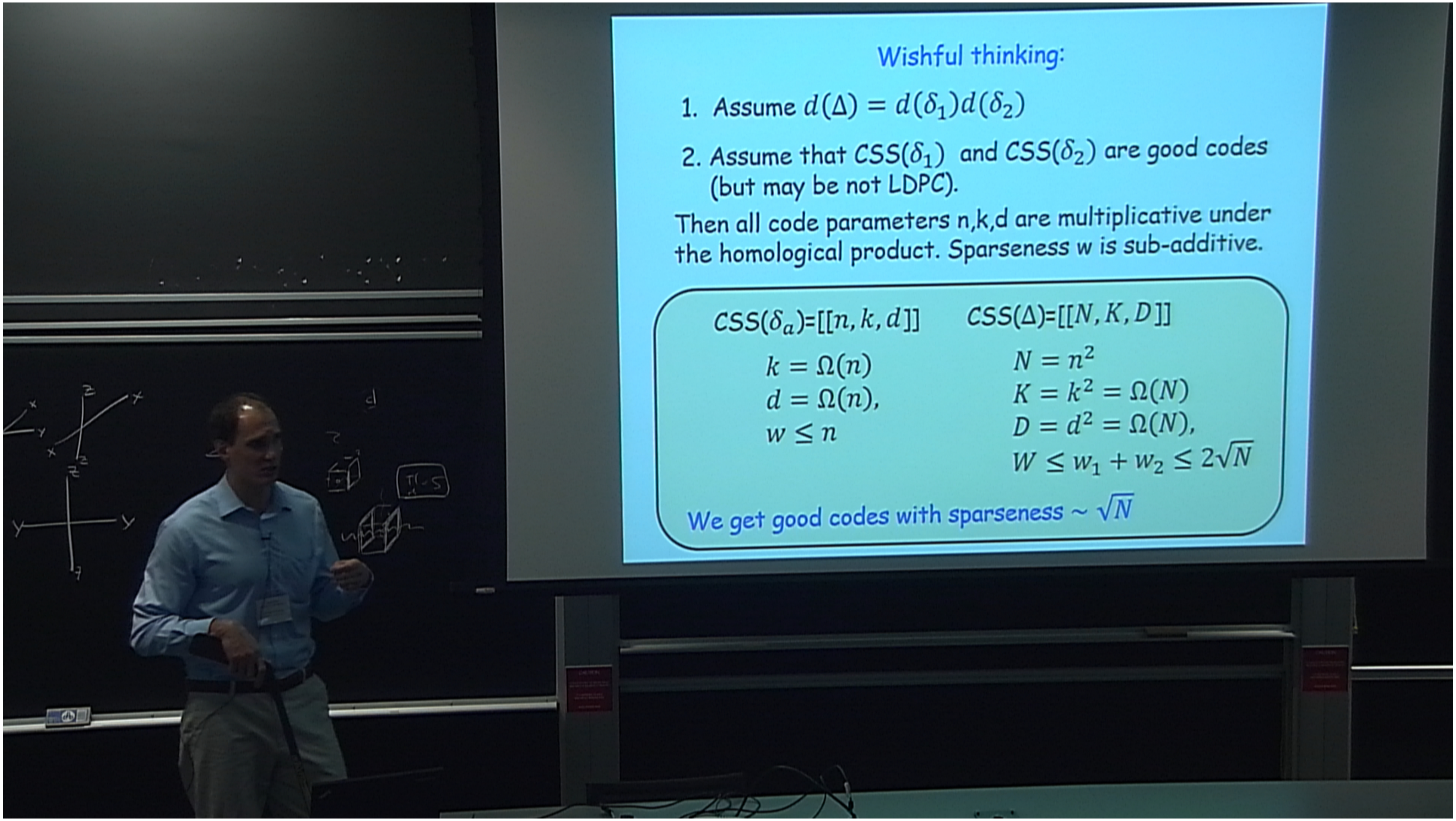

Sparse boundary operators from homology
⇨ Linear space of cells (simplexes) $C$
⇨ Boundary operator $\delta : C \to C$
The boundary of n-cell is a sum of (n-1)-cells:
2
1
3
$\delta(123) = (12) + (23) + (13)$
$\delta(12) = (1) + (2)$ etc
$\delta(1) = \delta(2) = \delta(3) = 0$

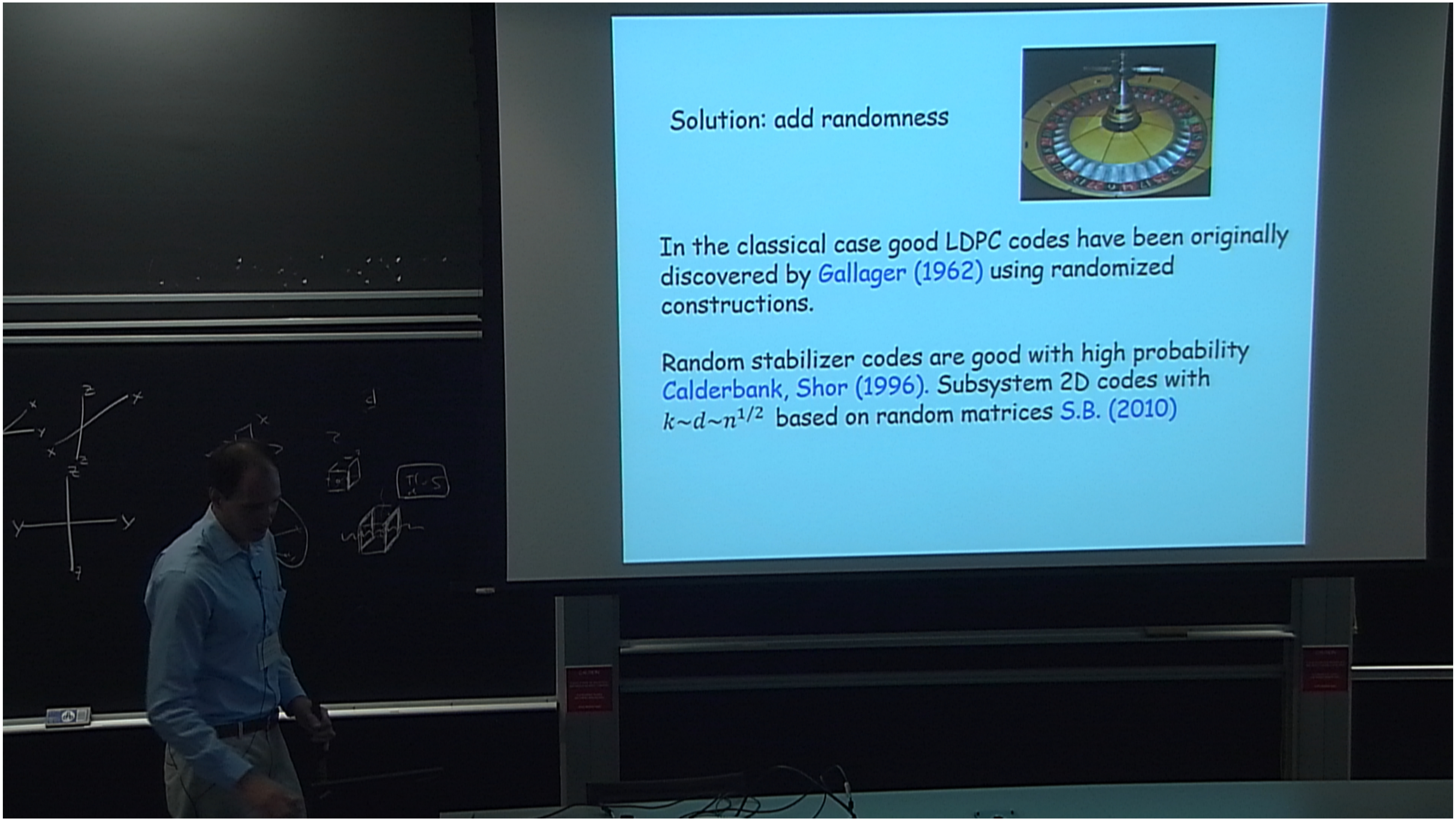

Homological product
$M_1$
$M_2$
$\delta_1 : C_1 \rightarrow C_1$
$\delta_2 : C_2 \rightarrow C_2$

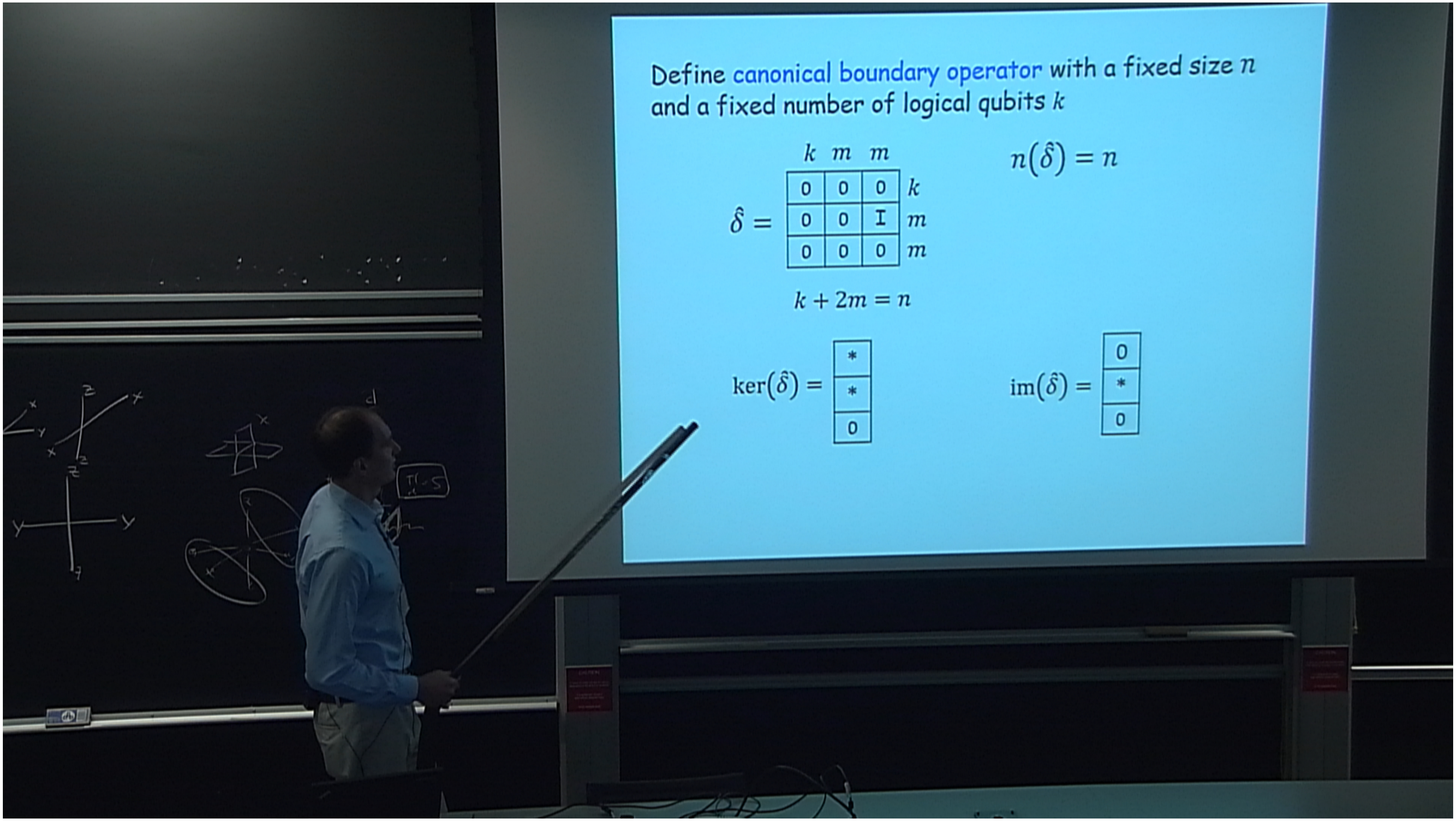

Homological product
$M_1$
$\times$
$M_2$
$\delta_1 : C_1 \to C_1$
$\delta_2 : C_2 \to C_2$
The product manifold $M = M_1 \times M_2$ has a linear space of cells $C = C_1 \otimes C_2$ and a boundary operator $\Delta : C \to C$
$\Delta = \delta_1 \otimes I + I \otimes \delta_2$
$\Delta^2 = (\delta_1)^2 \otimes I + 2\,\delta_1 \otimes \delta_2 + I \otimes (\delta_2)^2 = 0 \pmod 2$

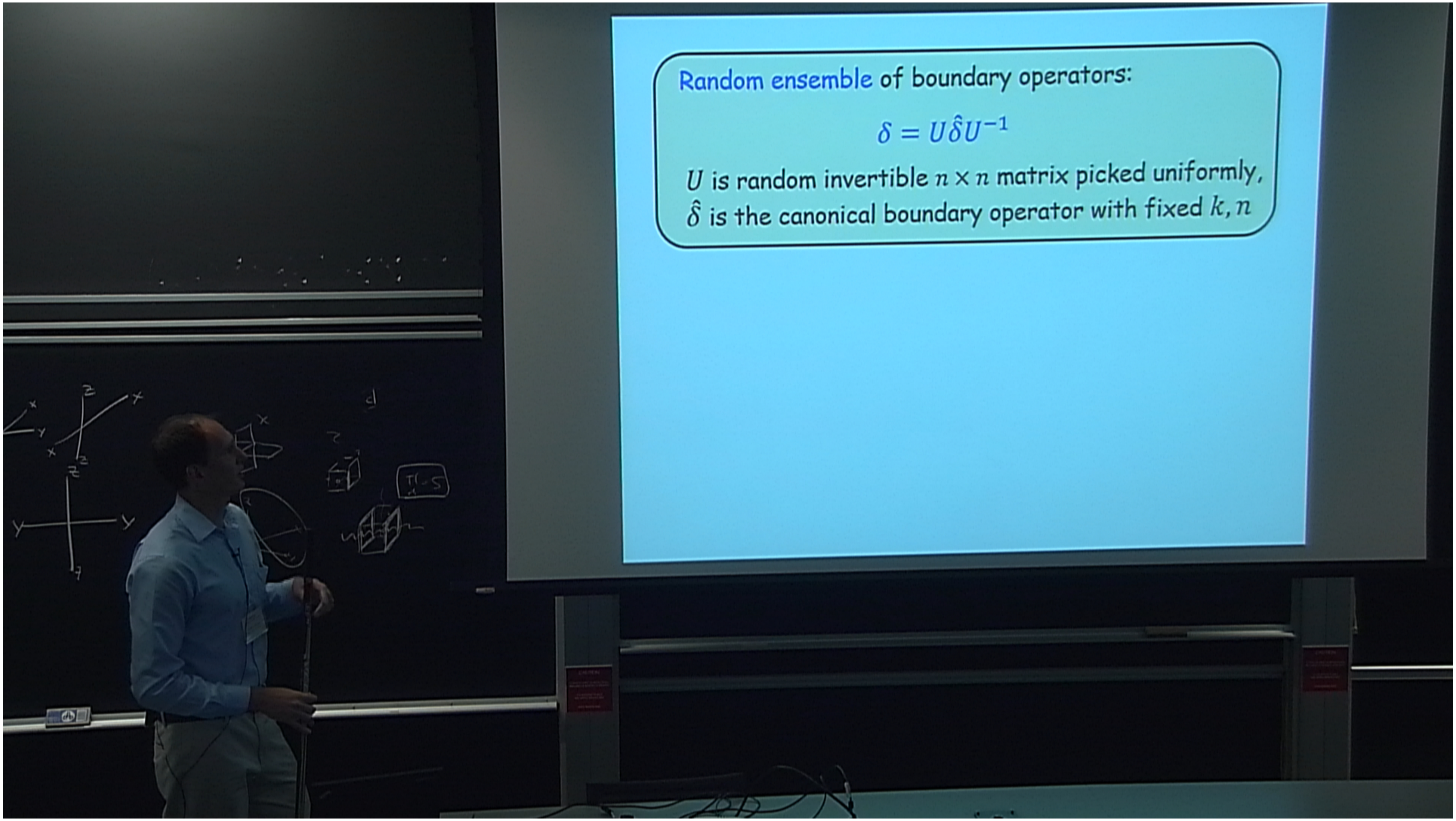

$\Delta = \delta_1 \otimes I + I \otimes \delta_2$
Parameters of the code $CSS(\Delta)$:
Number of code qubits: $n(\Delta) = n(\delta_1)n(\delta_2)$

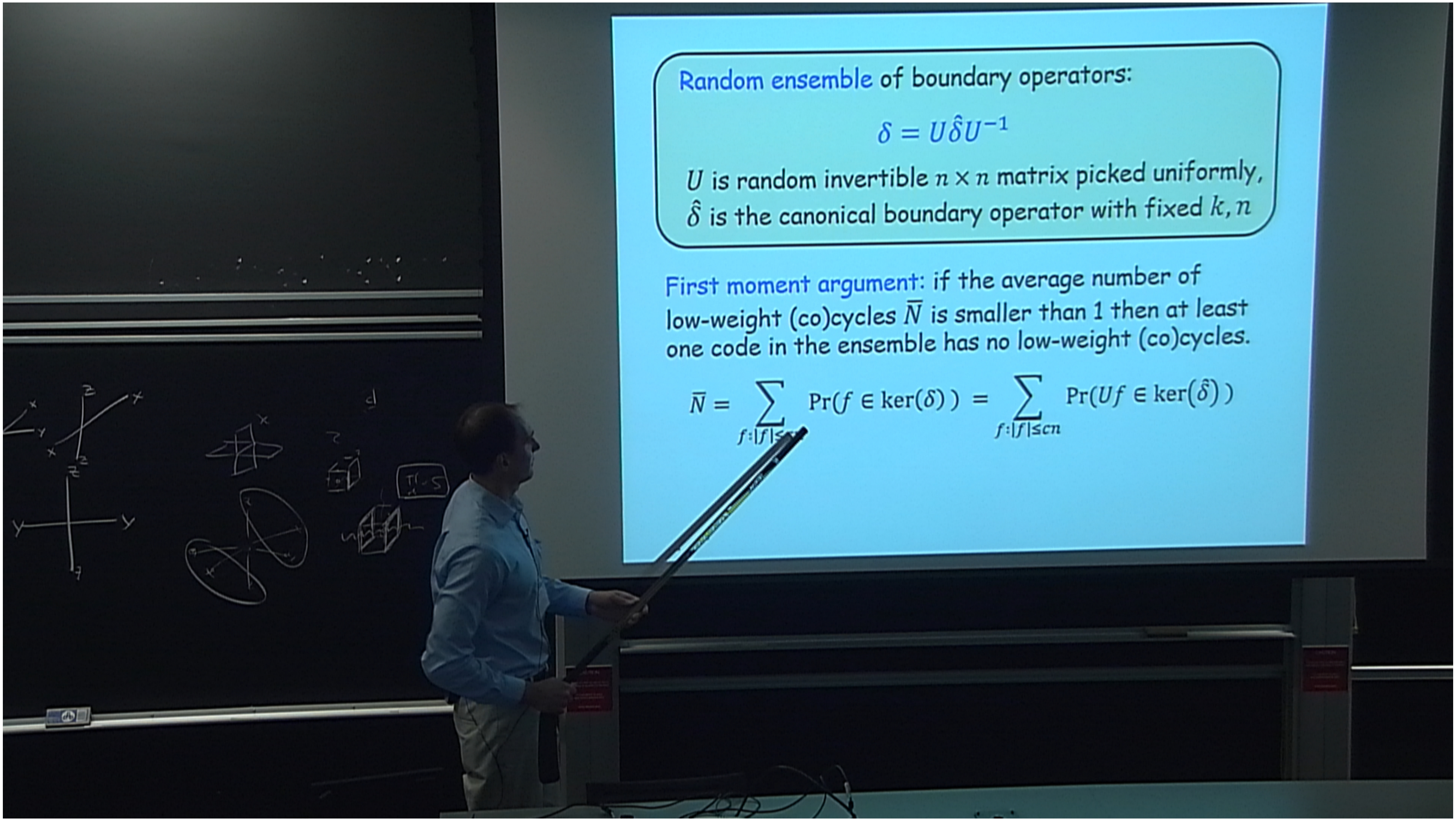

Wishful thinking:
1. Assume $d(\Delta) = d(\delta_1)d(\delta_2)$
2. Assume that $CSS(\delta_1)$ and $CSS(\delta_2)$ are good codes (but may be not LDPC).

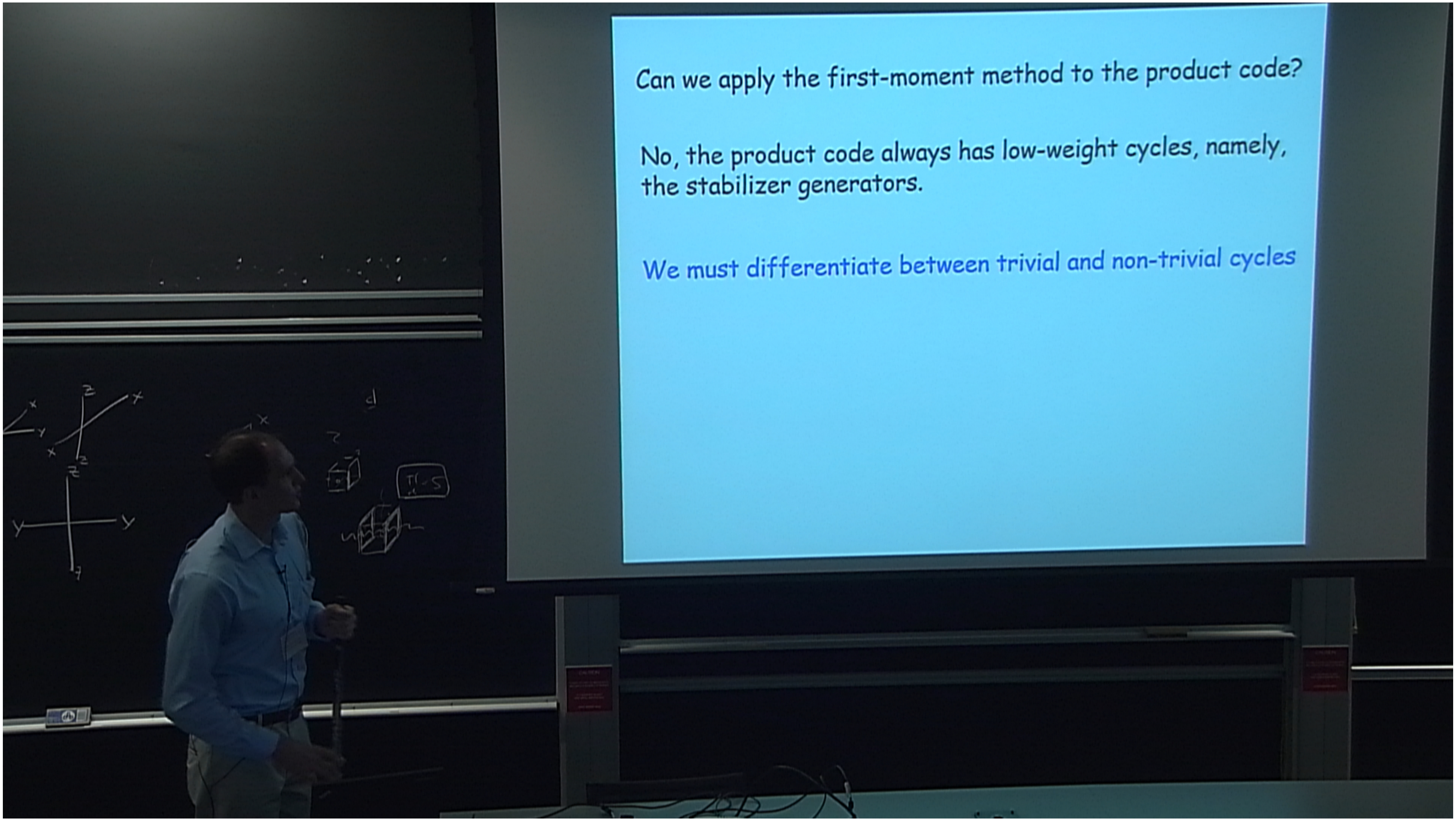

Wishful thinking:
1. Assume $d(\Delta) = d(\delta_1)d(\delta_2)$
2. Assume that $CSS(\delta_1)$ and $CSS(\delta_2)$ are good codes (but may be not LDPC).
Then all code parameters n,k,d are multiplicative under the homological product. Sparseness w is sub-additive.
$CSS(\delta_a)$=[[$n, k, d$]]
$k = \Omega(n)$
$d = \Omega(n)$,
$w \leq n$
$CSS(\Delta)$=[[$N, K, D$]]
$N = n^2$
$K = k^2 = \Omega(N)$
$D = d^2 = \Omega(N)$,
$W \leq w_1 + w_2 \leq 2\sqrt{N}$
We get good codes with sparseness $\sim \sqrt{N}$

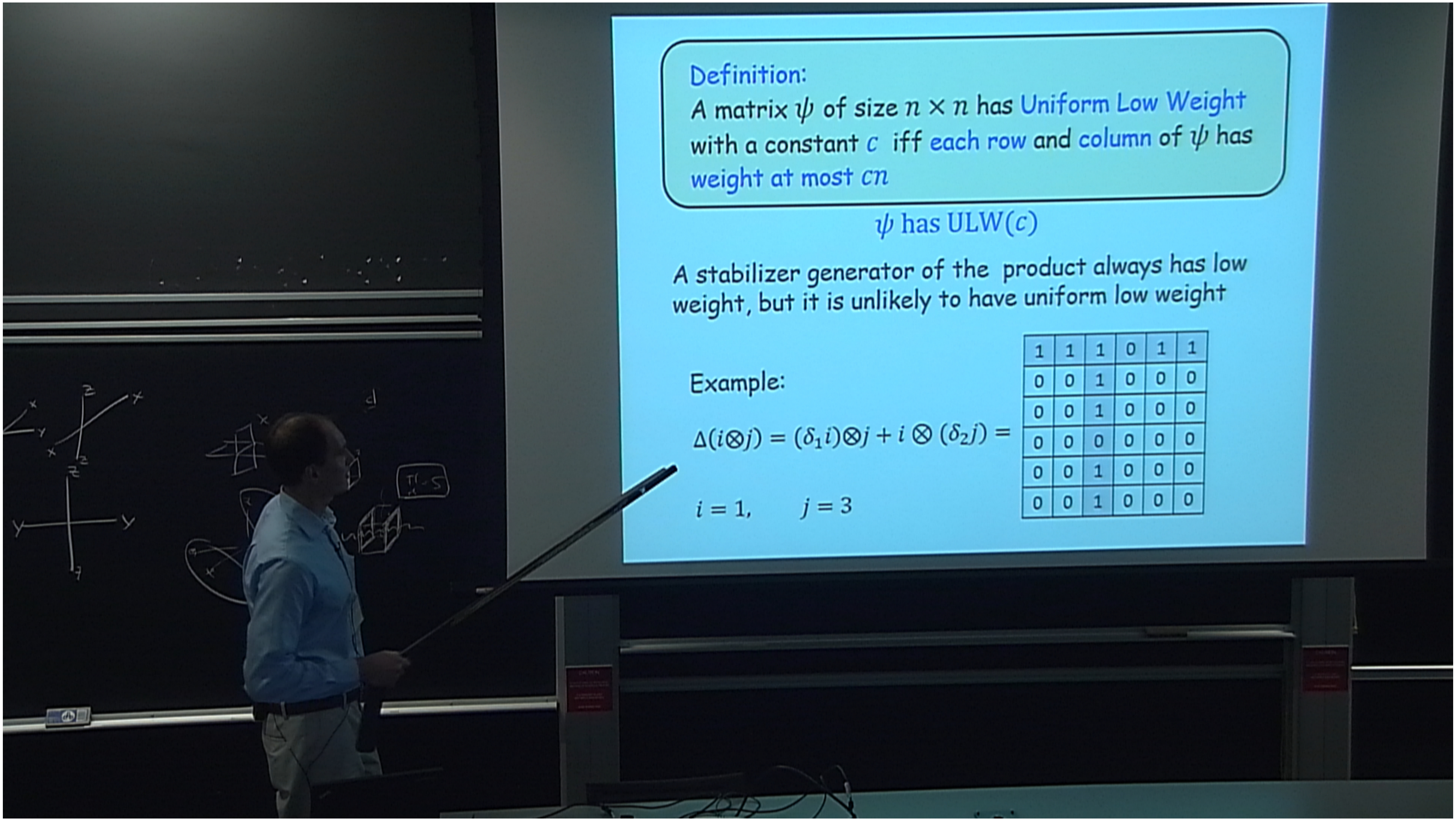

Solution: add randomness
In the classical case good LDPC codes have been originally discovered by Gallager (1962) using randomized constructions.
Random stabilizer codes are good with high probability Calderbank, Shor (1996). Subsystem 2D codes with $k \sim d \sim n^{1/2}$ based on random matrices S.B. (2010)

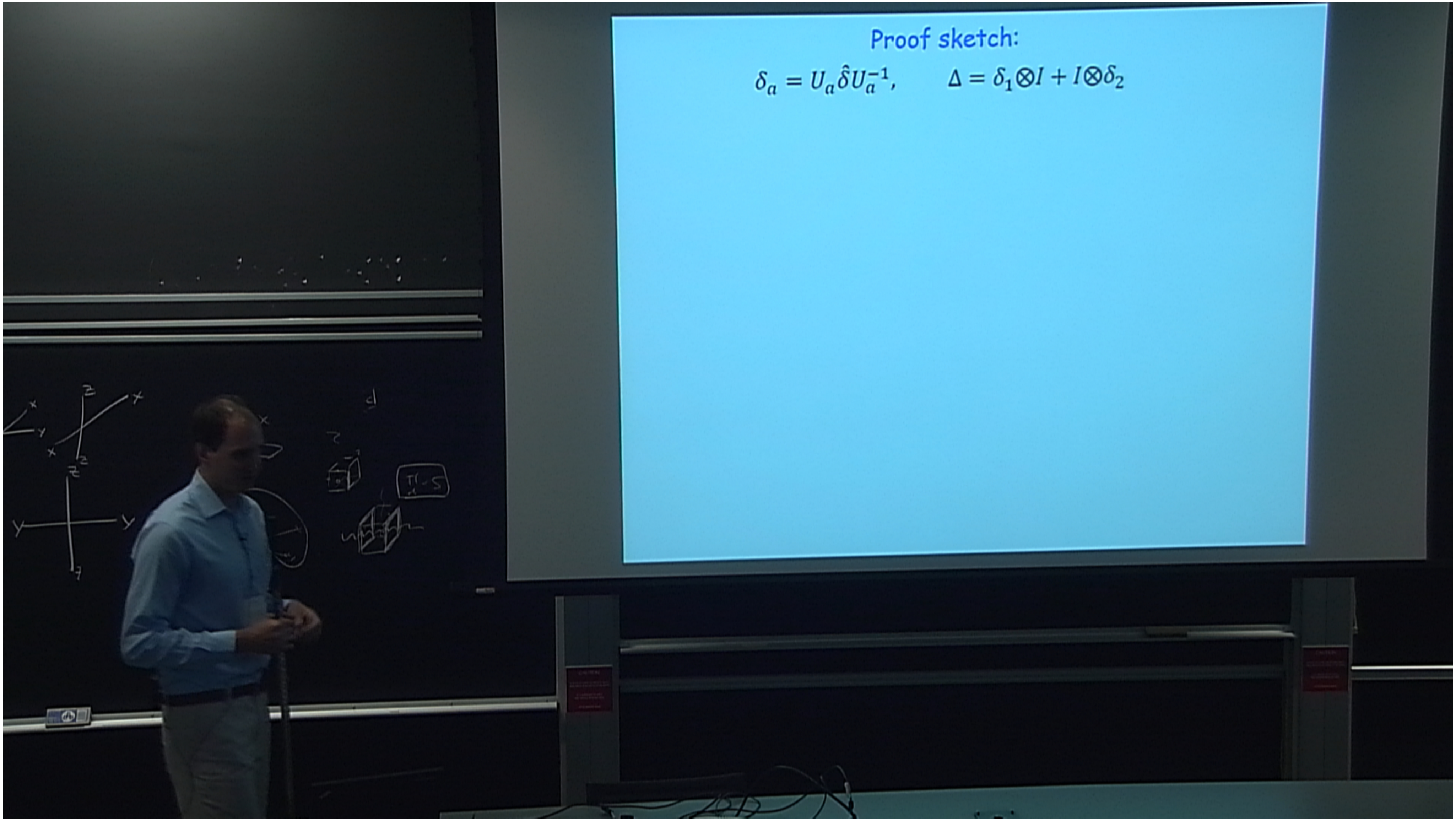

Define canonical boundary operator with a fixed size n and a fixed number of logical qubits k
k m m
δ̂ =
0 0 0 k
0 0 I m
0 0 0 m
n(δ̂) = n
k + 2m = n
ker(δ̂) =
*
*
0
im(δ̂) =
0
*
0

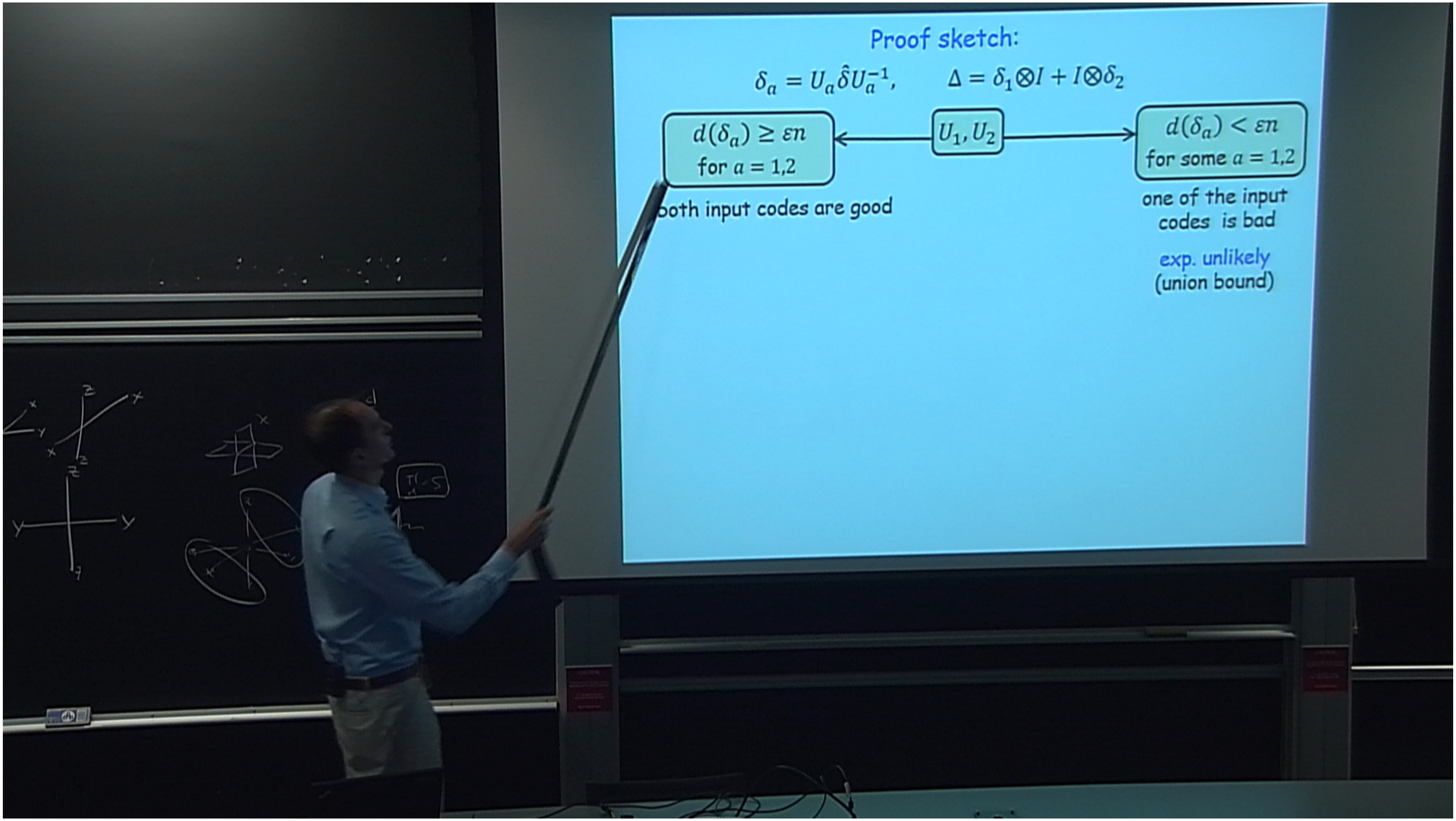

Random ensemble of boundary operators:
$\delta = U\hat{\delta}U^{-1}$
$U$ is random invertible $n \times n$ matrix picked uniformly,
$\hat{\delta}$ is the canonical boundary operator with fixed $k, n$

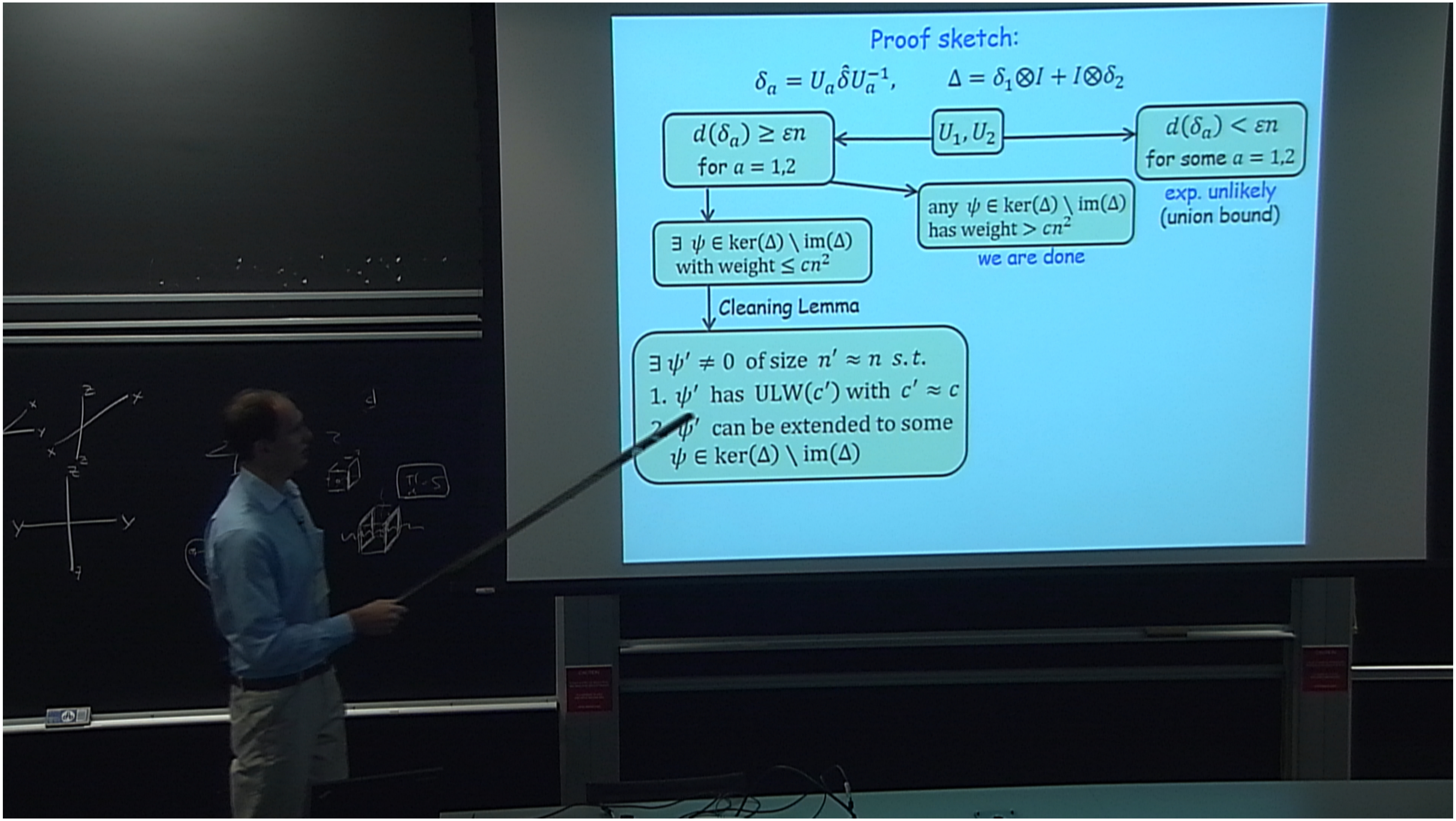

Random ensemble of boundary operators:
$\delta = U\hat{\delta}U^{-1}$
$U$ is random invertible $n \times n$ matrix picked uniformly,
$\hat{\delta}$ is the canonical boundary operator with fixed $k, n$
First moment argument: if the average number of
low-weight (co)cycles $\bar{N}$ is smaller than 1 then at least
one code in the ensemble has no low-weight (co)cycles.
$\bar{N} = \sum_{f:|f|\le} \Pr(f \in \ker(\delta)) = \sum_{f:|f|\le cn} \Pr(Uf \in \ker(\hat{\delta}))$

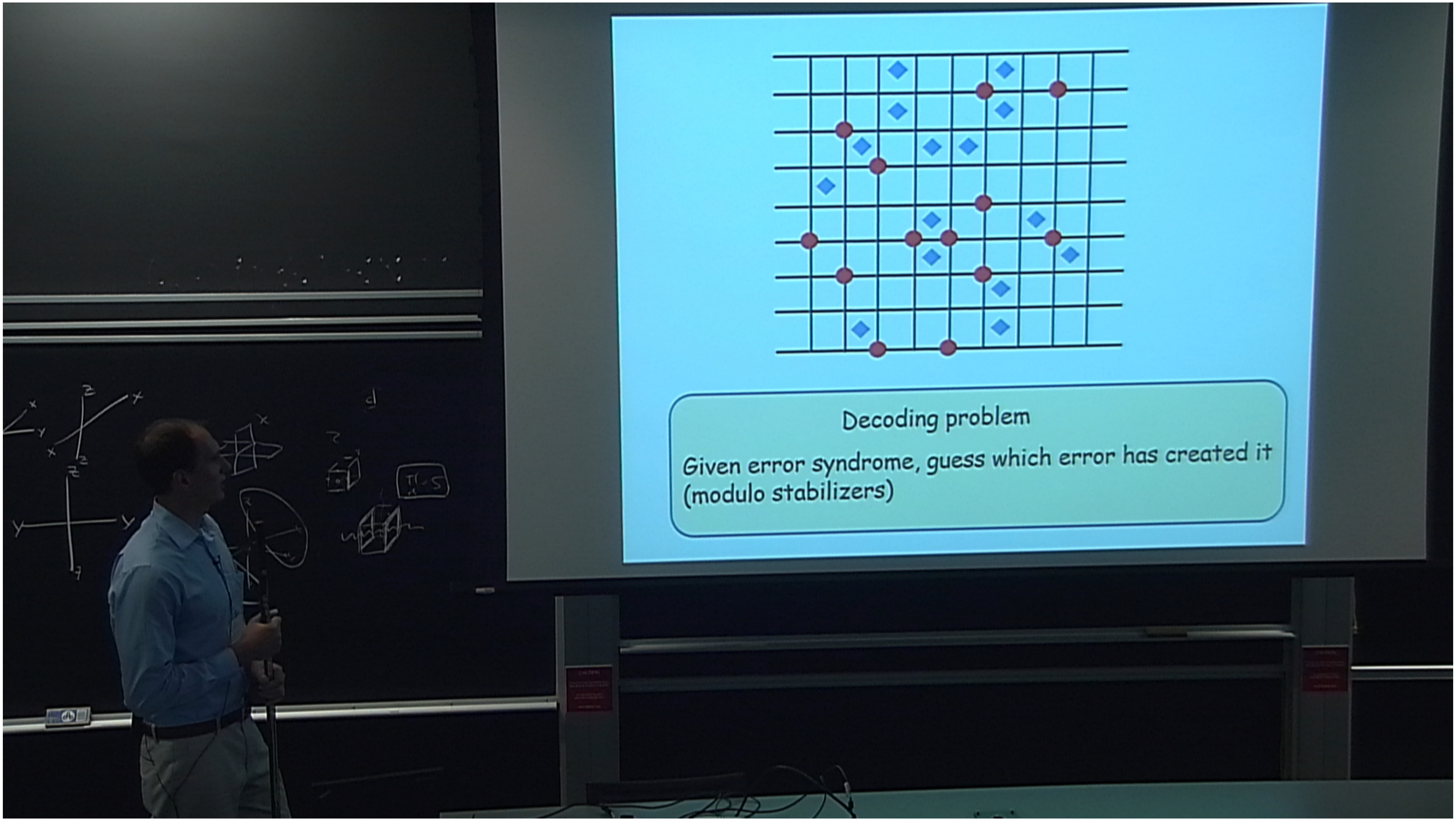

Can we apply the first-moment method to the product code?
No, the product code always has low-weight cycles, namely, the stabilizer generators.
We must differentiate between trivial and non-trivial cycles

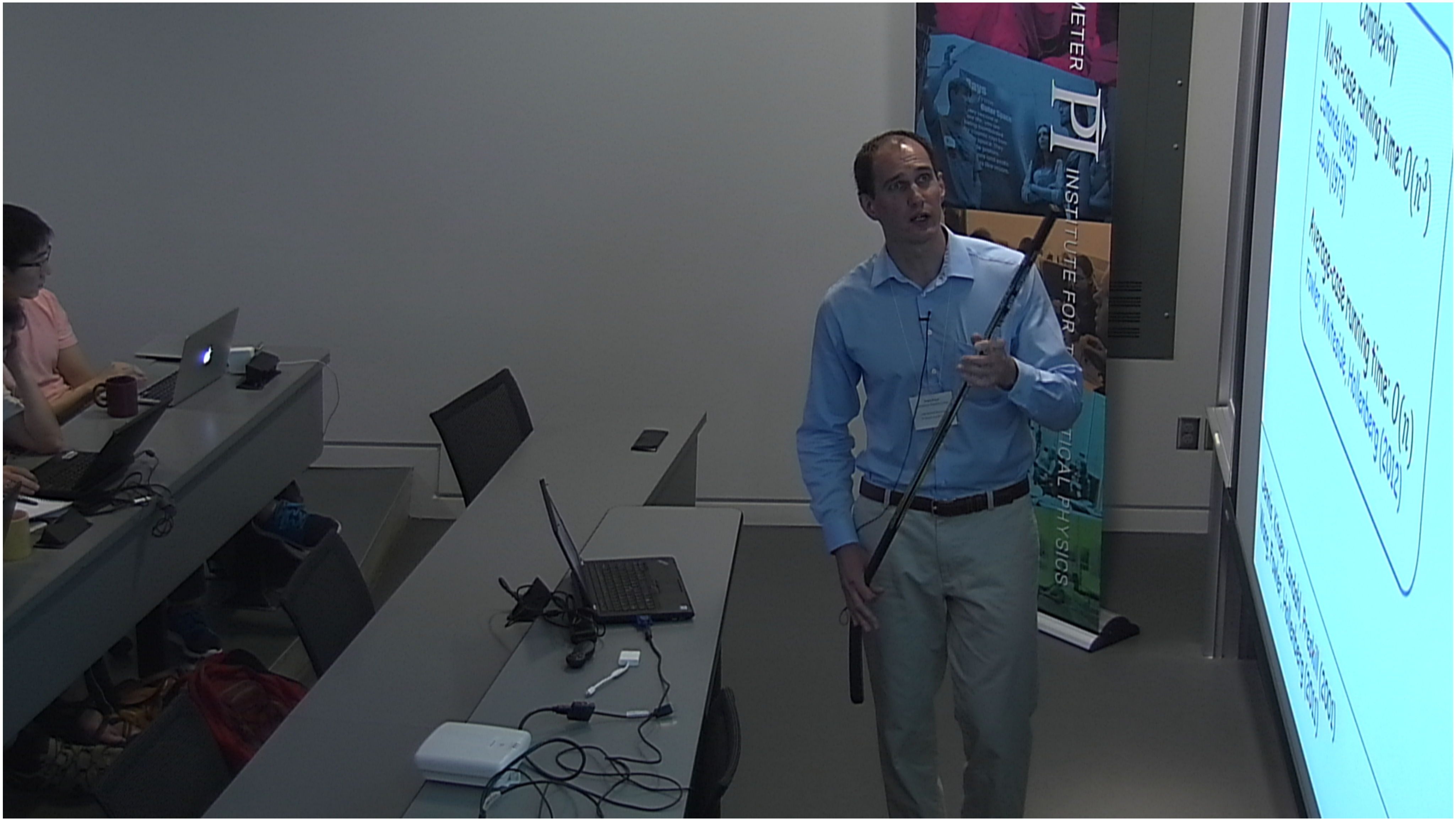

Definition:
A matrix ψ of size n × n has Uniform Low Weight with a constant c iff each row and column of ψ has weight at most cn
ψ has ULW(c)
A stabilizer generator of the product always has low weight, but it is unlikely to have uniform low weight
Example:
Δ(i⊗j) = (δ1 i)⊗j + i ⊗ (δ2 j) =
i = 1,   j = 3
1 1 1 0 1 1
0 0 1 0 0 0
0 0 1 0 0 0
0 0 0 0 0 0
0 0 1 0 0 0
0 0 1 0 0 0

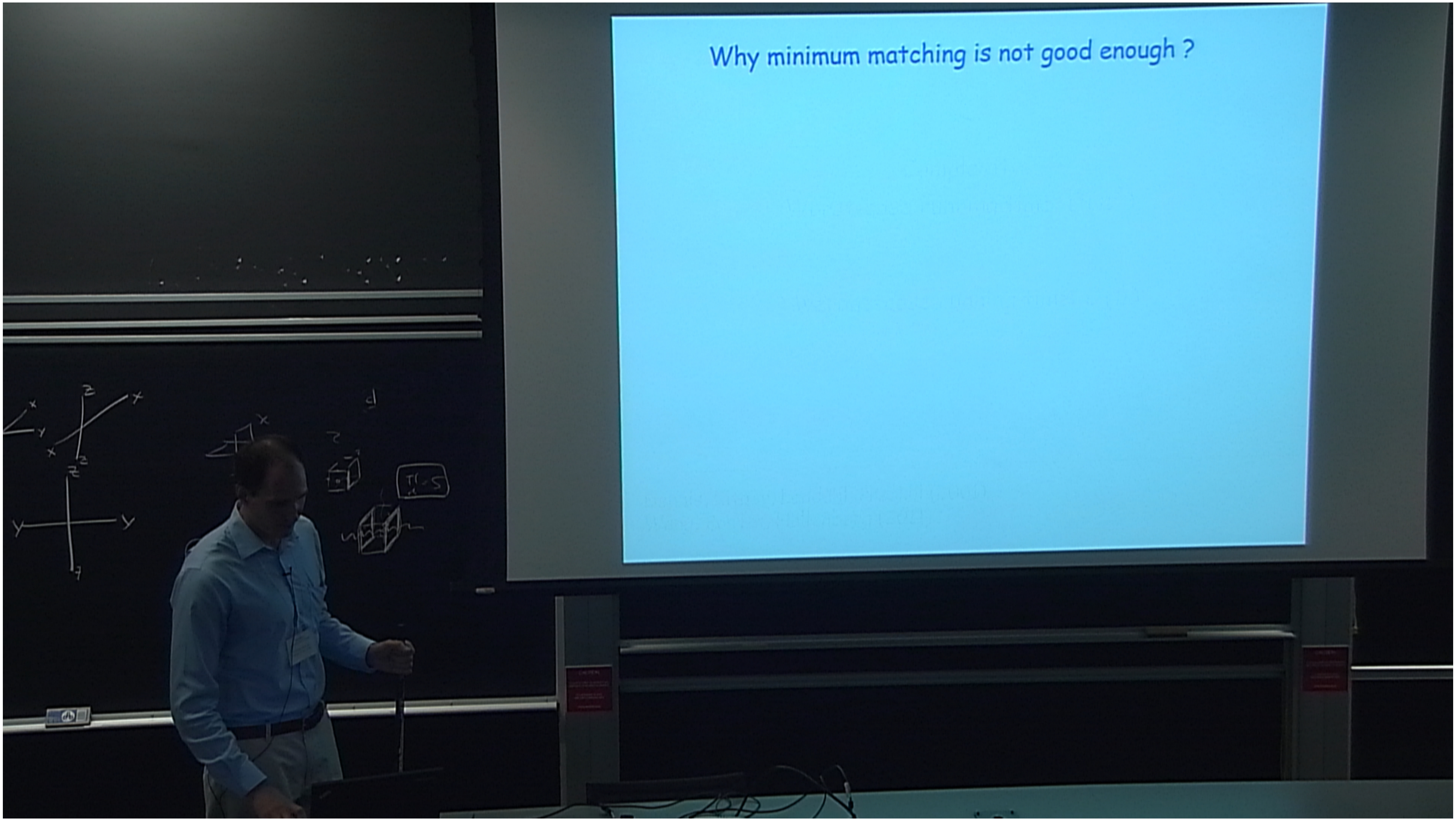

Proof sketch:
$\delta_a = U_a \hat{\delta} U_a^{-1}, \qquad \Delta = \delta_1 \otimes I + I \otimes \delta_2$

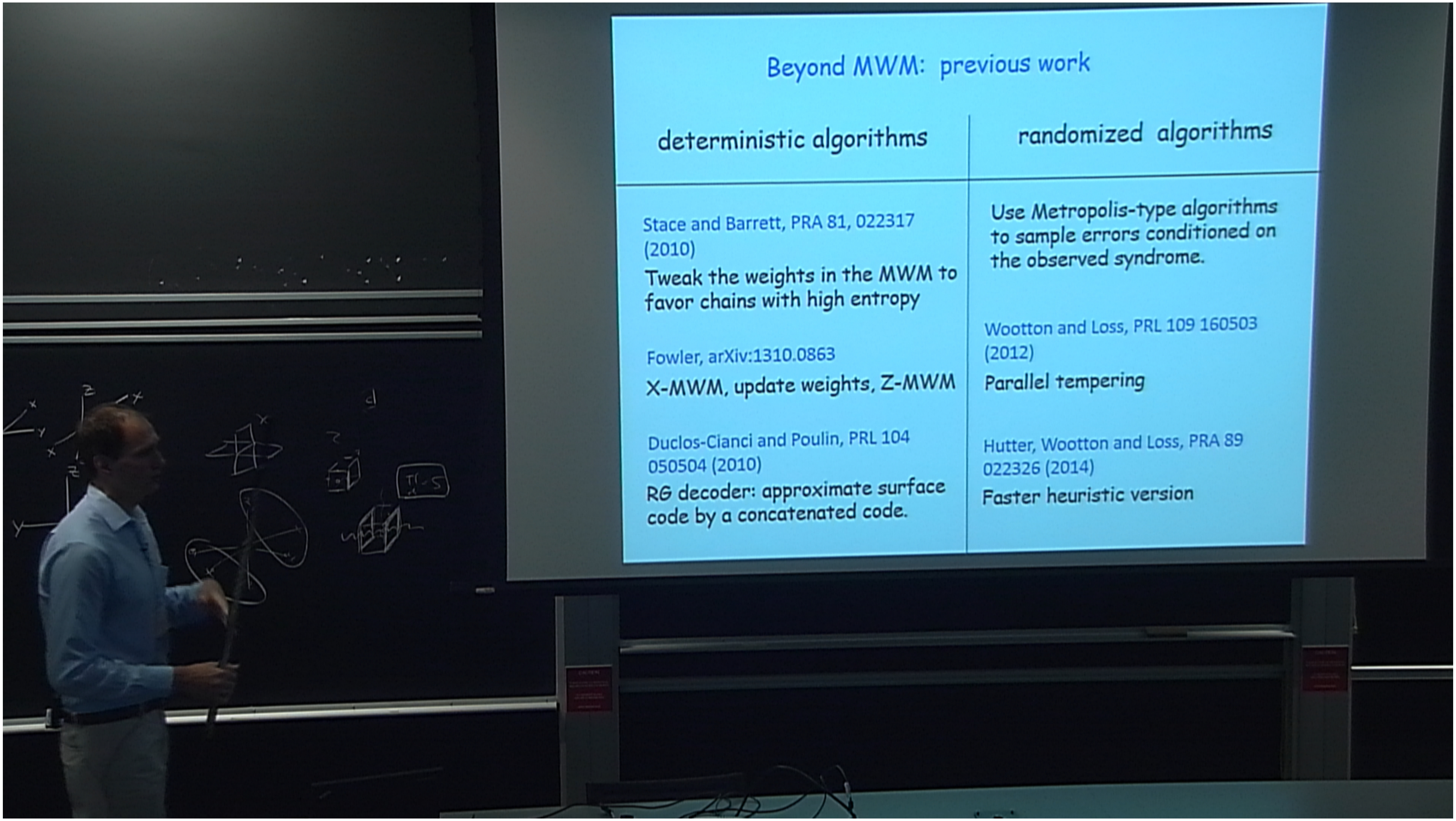

Proof sketch:
$\delta_a = U_a \hat{\delta} U_a^{-1}$,
$\Delta = \delta_1 \otimes I + I \otimes \delta_2$
$d(\delta_a) \geq \varepsilon n$
for $a = 1,2$
$U_1, U_2$
$d(\delta_a) < \varepsilon n$
for some $a = 1,2$
both input codes are good
one of the input codes is bad
exp. unlikely
(union bound)

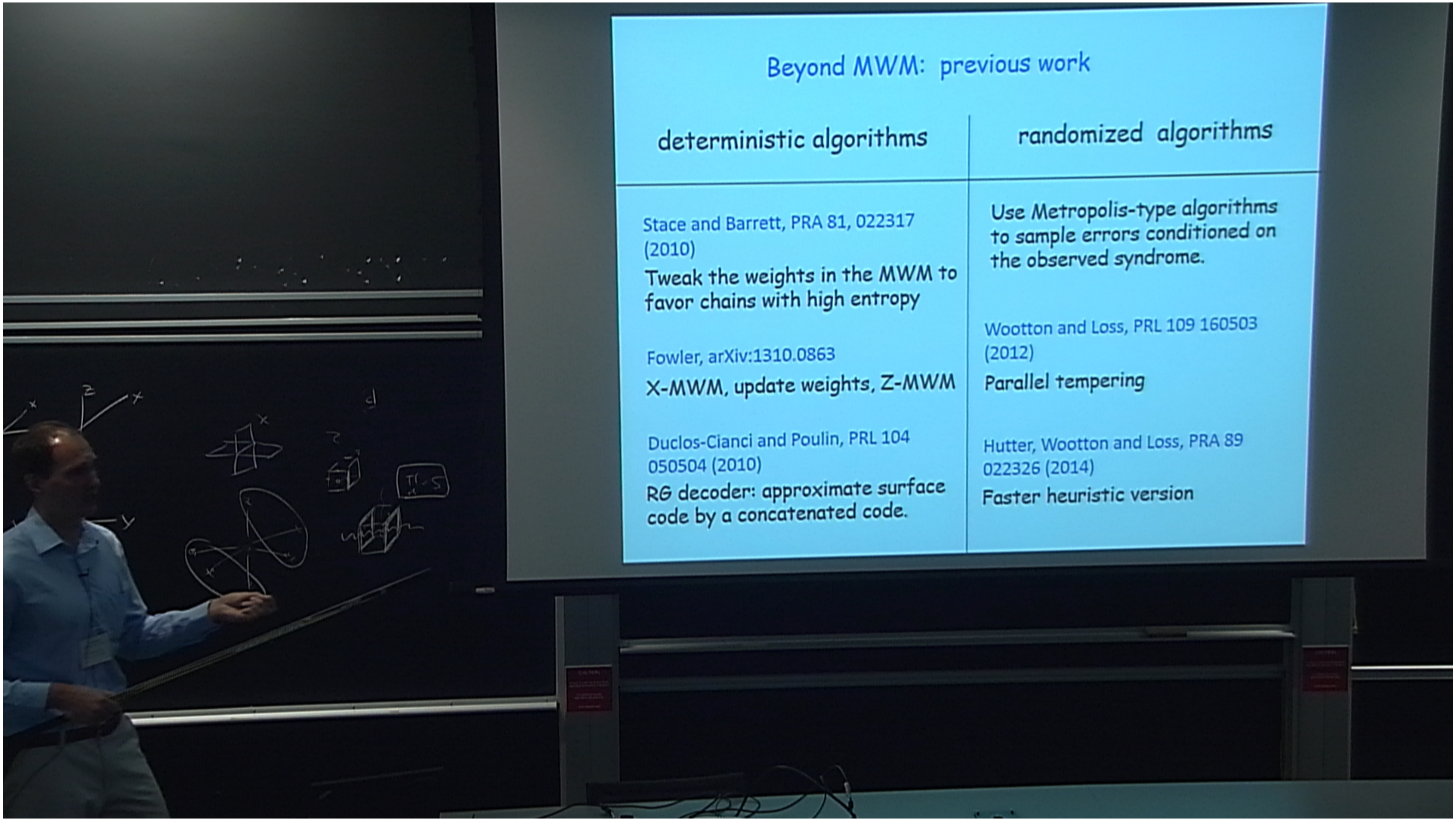

Proof sketch:
$\delta_a = U_a \hat{\delta} U_a^{-1}$,   $\Delta = \delta_1 \otimes I + I \otimes \delta_2$
$d(\delta_a) \geq \varepsilon n$ for $a = 1,2$
$U_1, U_2$
$d(\delta_a) < \varepsilon n$ for some $a = 1,2$
exp. unlikely (union bound)
any $\psi \in \ker(\Delta) \setminus \mathrm{im}(\Delta)$ has weight $> cn^2$
we are done
$\exists\ \psi \in \ker(\Delta) \setminus \mathrm{im}(\Delta)$ with weight $\leq cn^2$
Cleaning Lemma
$\exists\ \psi' \neq 0$ of size $n' \approx n$ s.t.
1. $\psi'$ has ULW($c'$) with $c' \approx c$
2. $\psi'$ can be extended to some $\psi \in \ker(\Delta) \setminus \mathrm{im}(\Delta)$

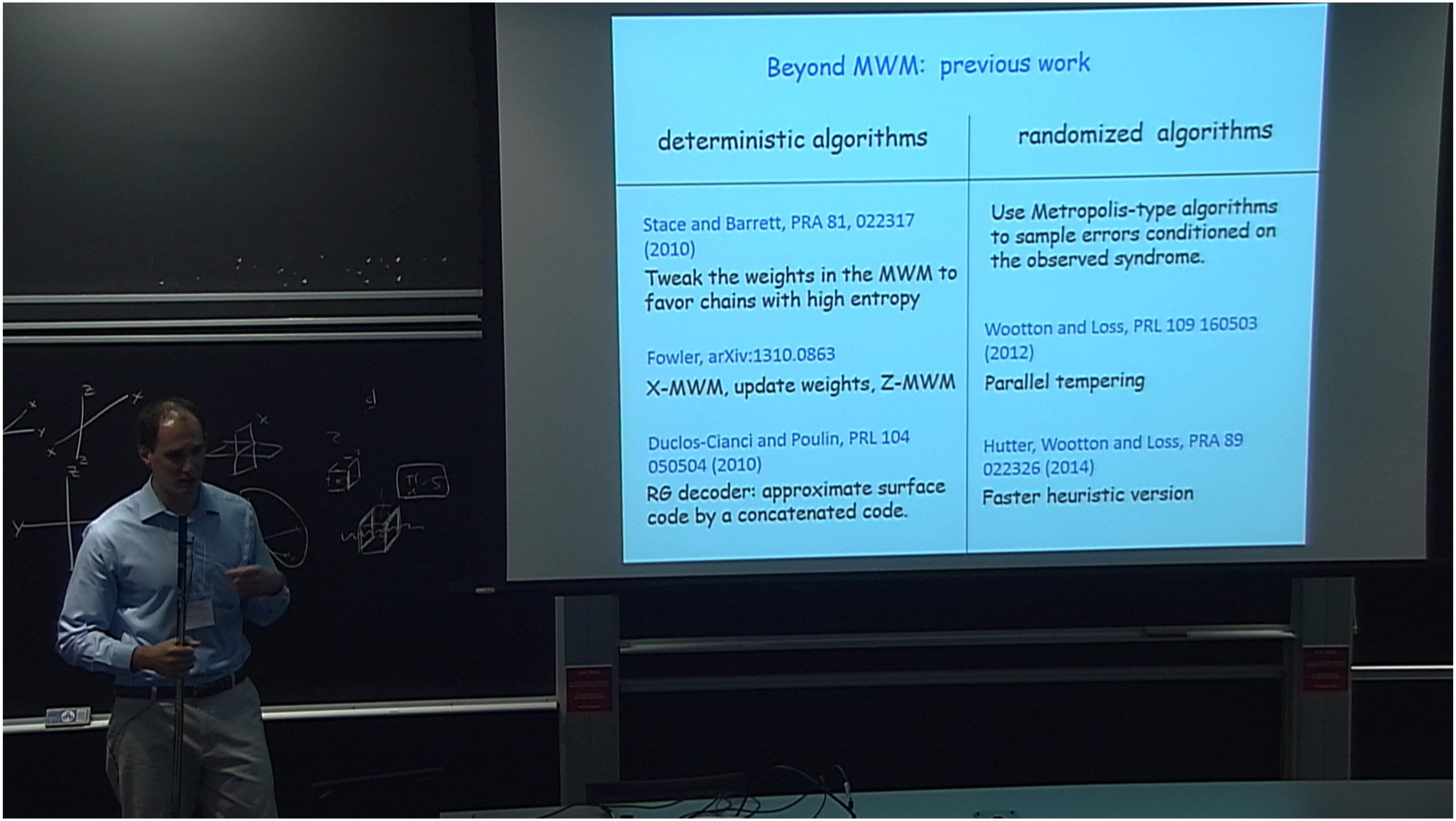

Decoding problem
Given error syndrome, guess which error has created it (modulo stabilizers)

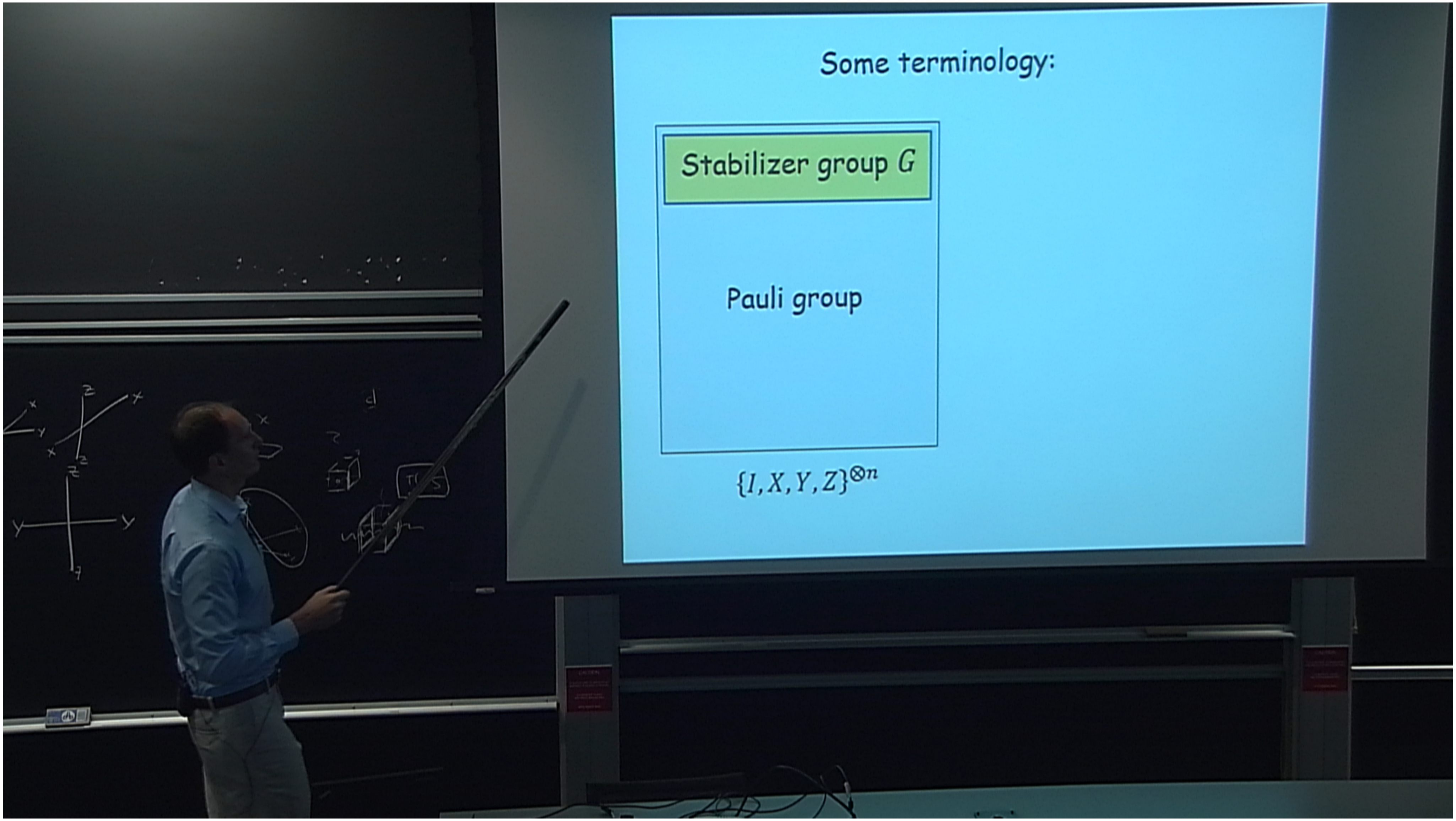

Complexity
Worst-case running time: O(n^3)
Edmonds (1965)
Gabow (1973)
Average-case running time: O(n)
Fowler, Whiteside, Hollenberg (2012)
INSTITUTE FOR
PHYSICS

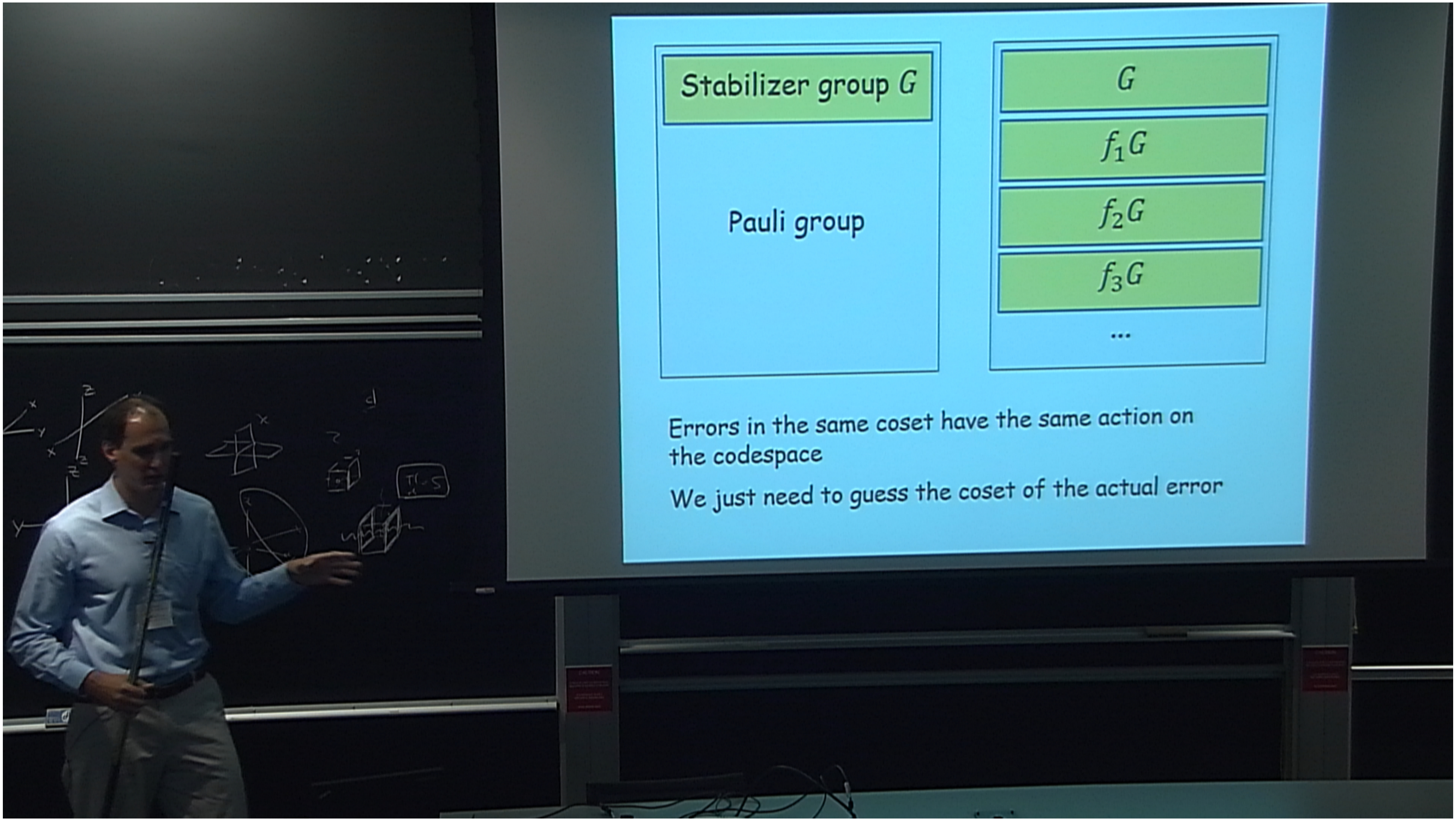

Why minimum matching is not good enough ?

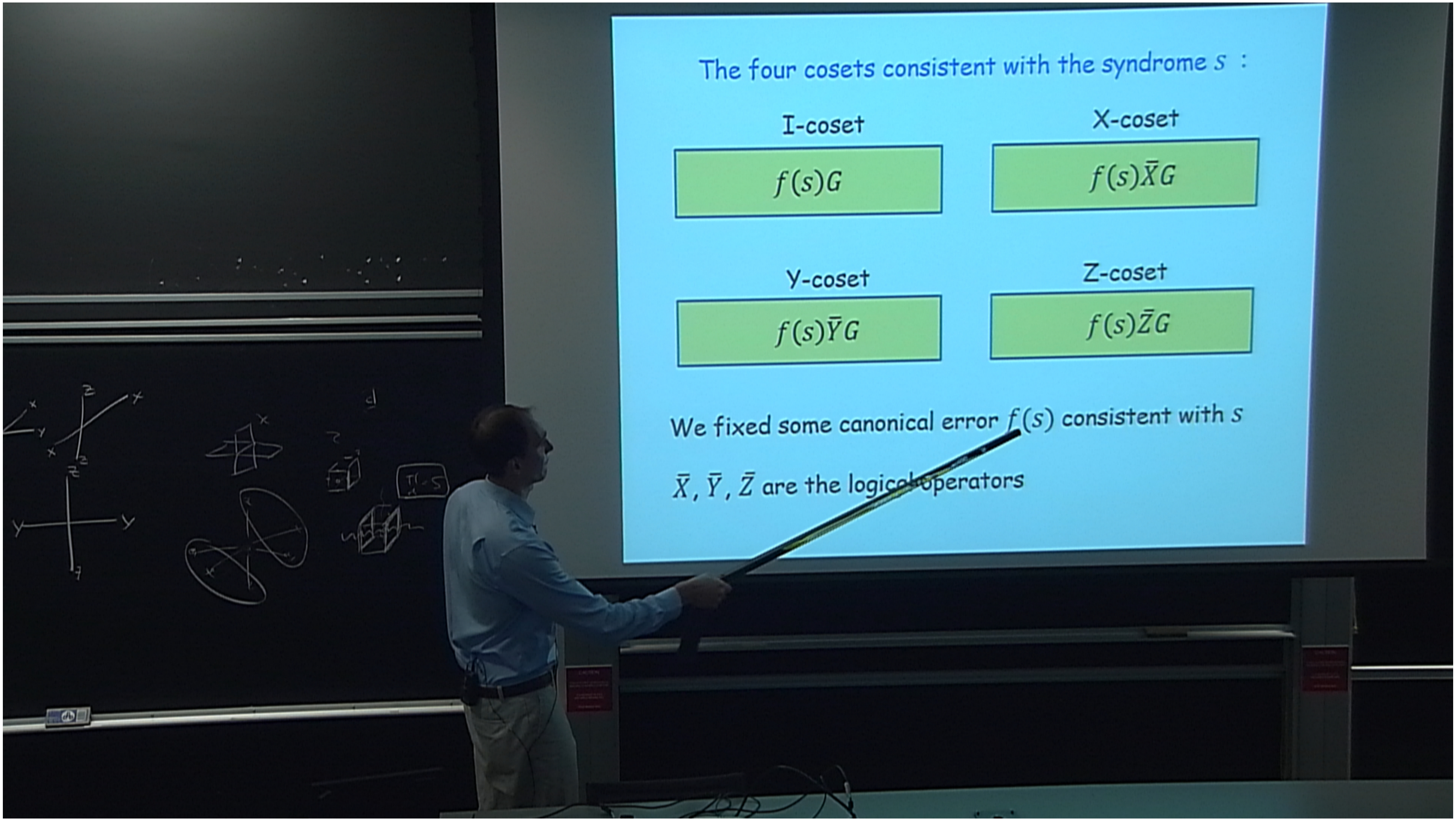

Beyond MWM: previous work
deterministic algorithms
randomized algorithms
Stace and Barrett, PRA 81, 022317 (2010)
Tweak the weights in the MWM to favor chains with high entropy
Fowler, arXiv:1310.0863
X-MWM, update weights, Z-MWM
Duclos-Cianci and Poulin, PRL 104 050504 (2010)
RG decoder: approximate surface code by a concatenated code.
Use Metropolis-type algorithms to sample errors conditioned on the observed syndrome.
Wootton and Loss, PRL 109 160503 (2012)
Parallel tempering
Hutter, Wootton and Loss, PRA 89 022326 (2014)
Faster heuristic version

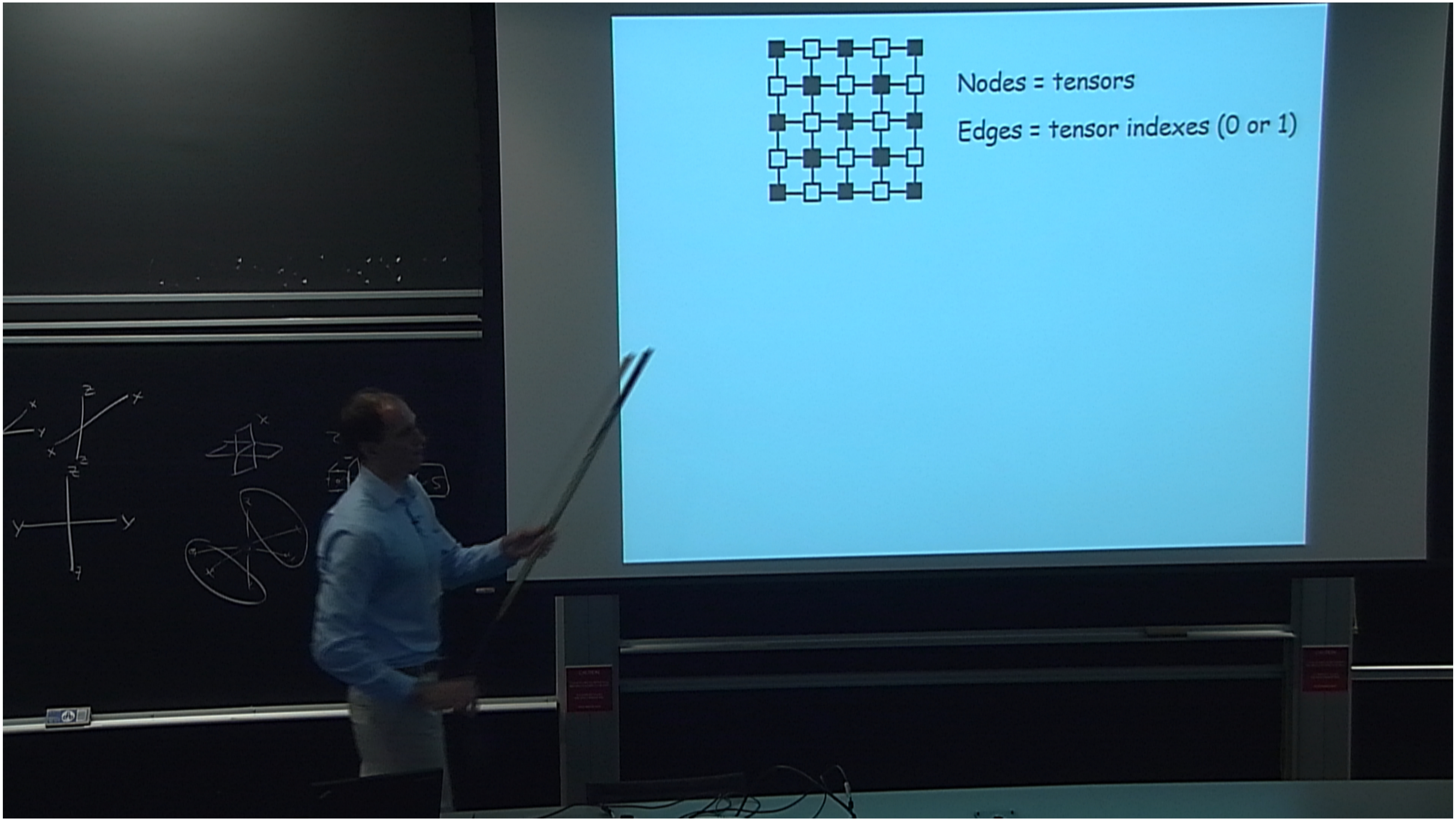

Beyond MWM: previous work
deterministic algorithms
randomized algorithms
Stace and Barrett, PRA 81, 022317 (2010)
Tweak the weights in the MWM to favor chains with high entropy
Fowler, arXiv:1310.0863
X-MWM, update weights, Z-MWM
Duclos-Cianci and Poulin, PRL 104 050504 (2010)
RG decoder: approximate surface code by a concatenated code.
Use Metropolis-type algorithms to sample errors conditioned on the observed syndrome.
Wootton and Loss, PRL 109 160503 (2012)
Parallel tempering
Hutter, Wootton and Loss, PRA 89 022326 (2014)
Faster heuristic version

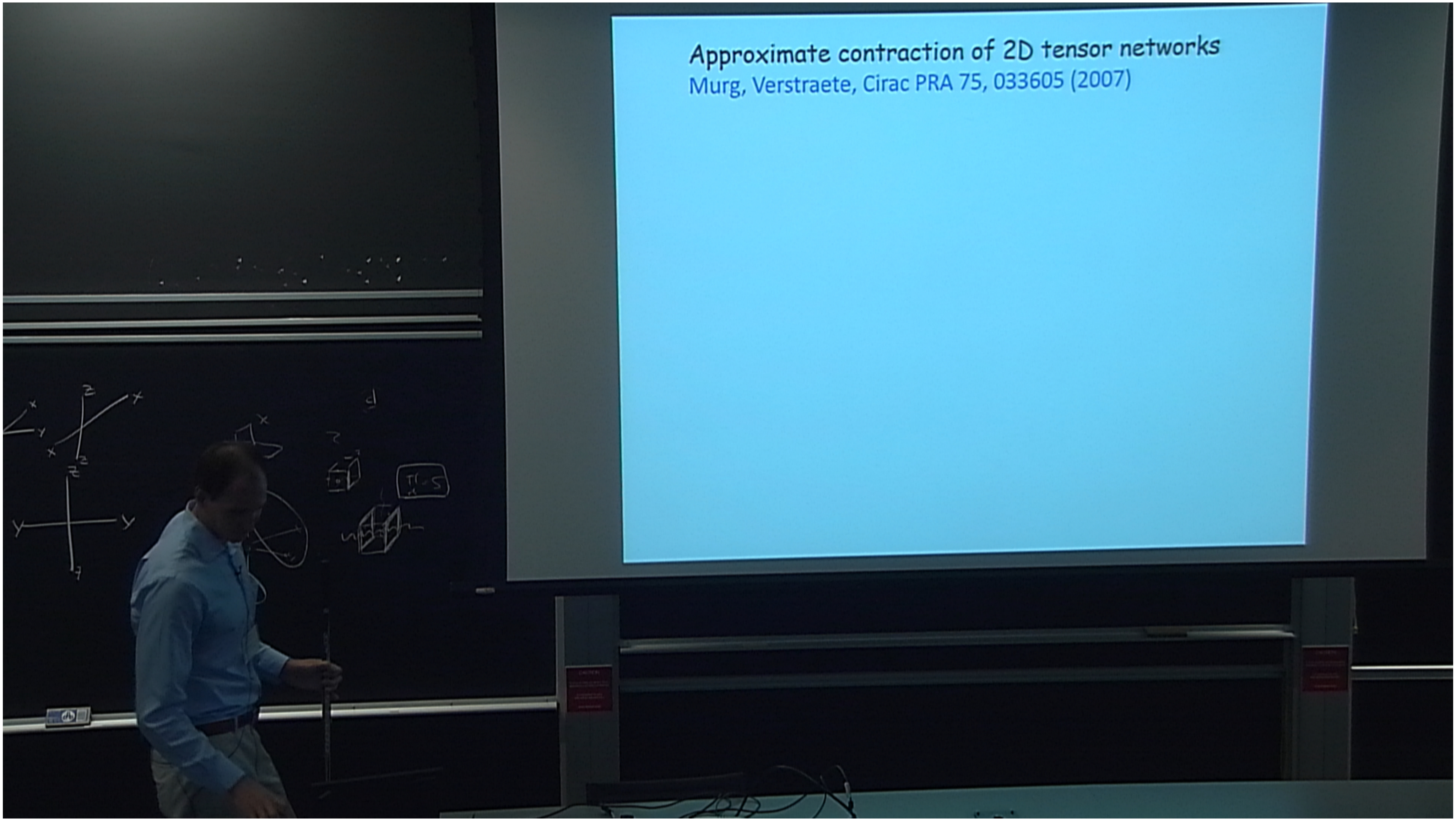

Beyond MWM: previous work
deterministic algorithms
randomized algorithms
Stace and Barrett, PRA 81, 022317 (2010)
Tweak the weights in the MWM to favor chains with high entropy
Fowler, arXiv:1310.0863
X-MWM, update weights, Z-MWM
Duclos-Cianci and Poulin, PRL 104 050504 (2010)
RG decoder: approximate surface code by a concatenated code.
Use Metropolis-type algorithms to sample errors conditioned on the observed syndrome.
Wootton and Loss, PRL 109 160503 (2012)
Parallel tempering
Hutter, Wootton and Loss, PRA 89 022326 (2014)
Faster heuristic version

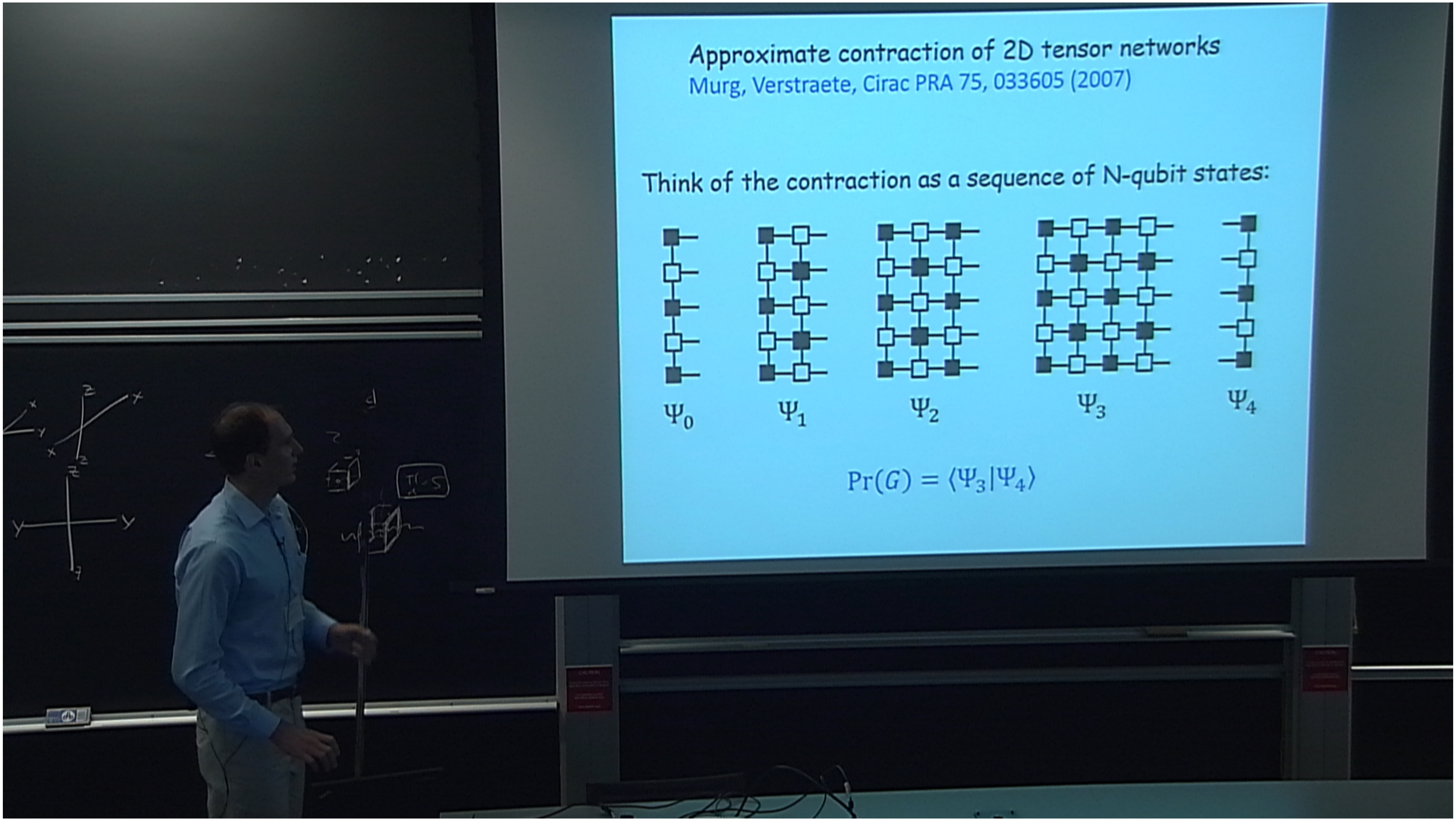

Some terminology:
Stabilizer group $G$
Pauli group
$\{I, X, Y, Z\}^{\otimes n}$

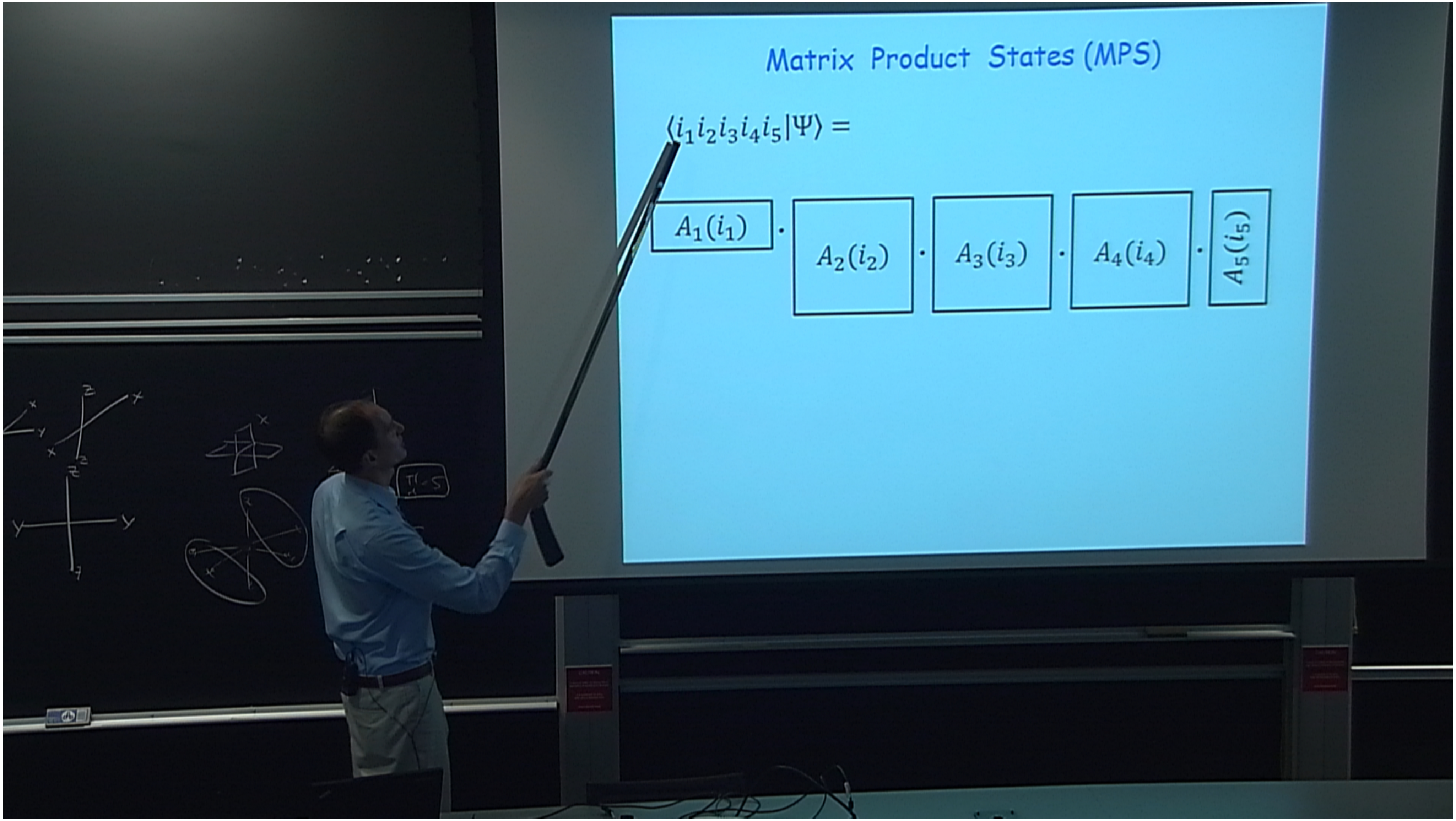

Stabilizer group $G$
Pauli group
$G$
$f_1G$
$f_2G$
$f_3G$
...
Errors in the same coset have the same action on the codespace
We just need to guess the coset of the actual error

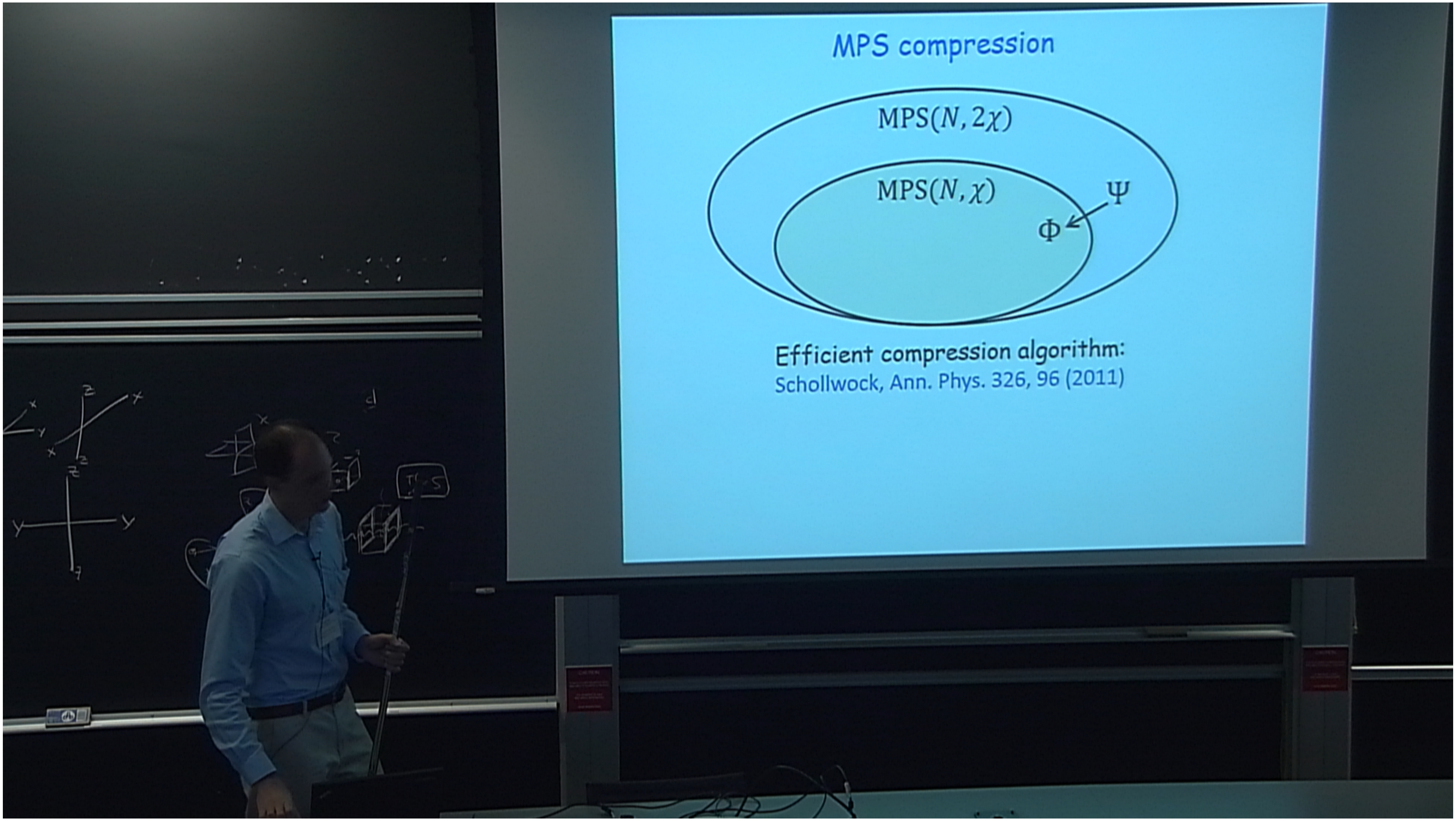

The four cosets consistent with the syndrome $s$ :
I-coset
$f(s)G$
X-coset
$f(s)\bar{X}G$
Y-coset
$f(s)\bar{Y}G$
Z-coset
$f(s)\bar{Z}G$
We fixed some canonical error $f(s)$ consistent with $s$
$\bar{X}, \bar{Y}, \bar{Z}$ are the logical operators

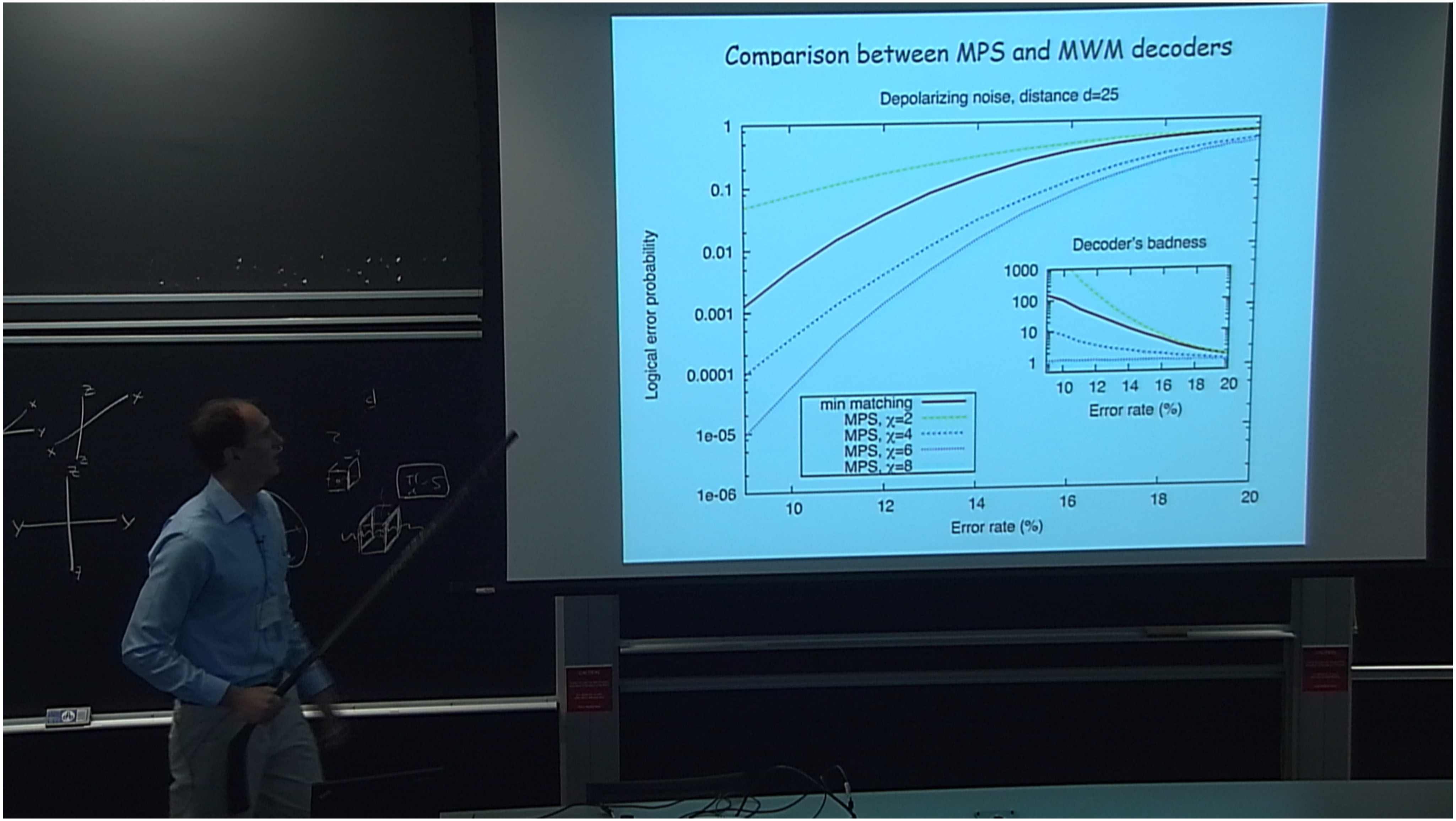

Nodes = tensors
Edges = tensor indexes (0 or 1)

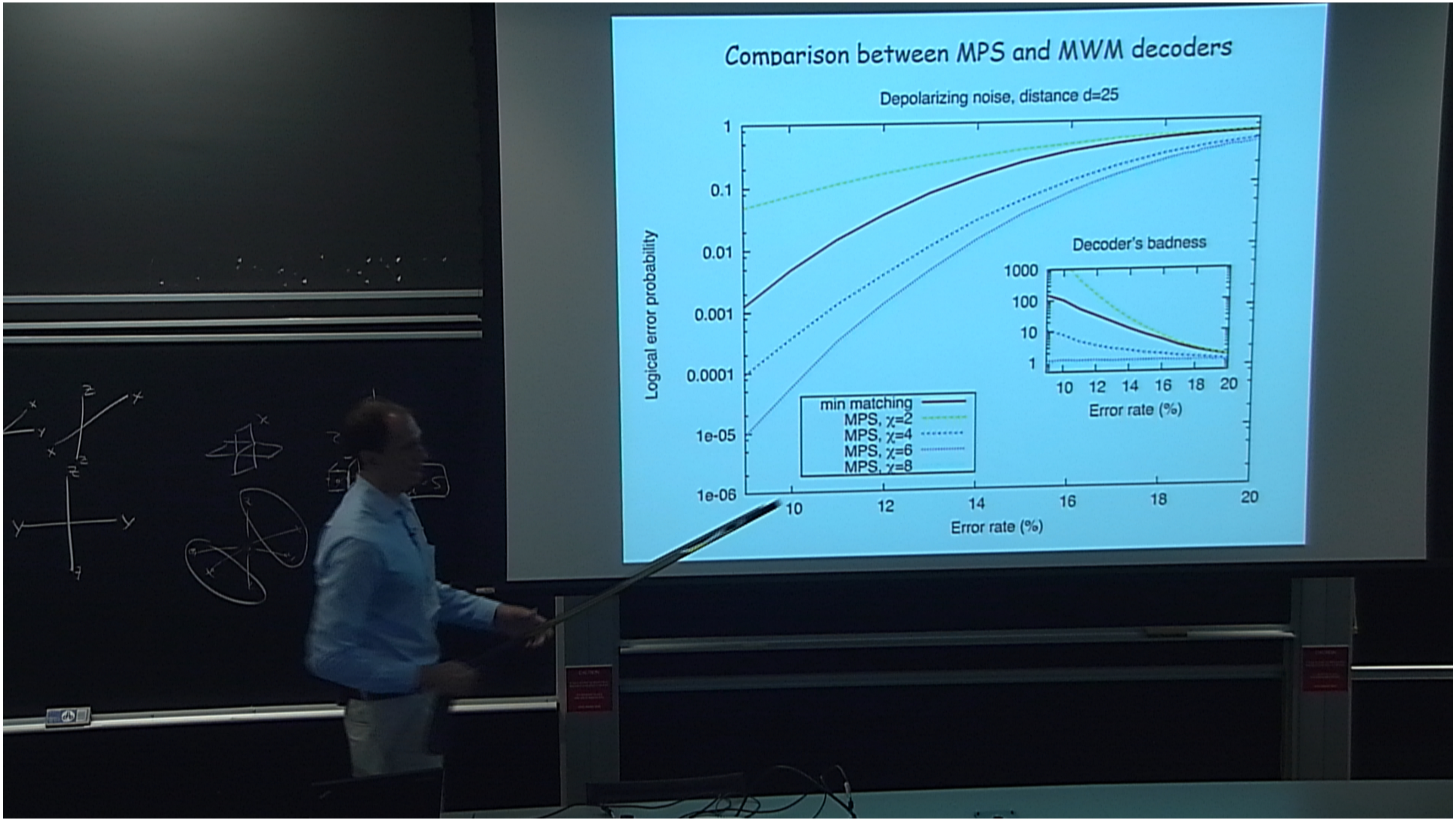

Approximate contraction of 2D tensor networks
Murg, Verstraete, Cirac PRA 75, 033605 (2007)


Approximate contraction of 2D tensor networks
Murg, Verstraete, Cirac PRA 75, 033605 (2007)
Think of the contraction as a sequence of N-qubit states:
Ψ0
Ψ1
Ψ2
Ψ3
Ψ4
Pr(G) = ⟨Ψ3|Ψ4⟩

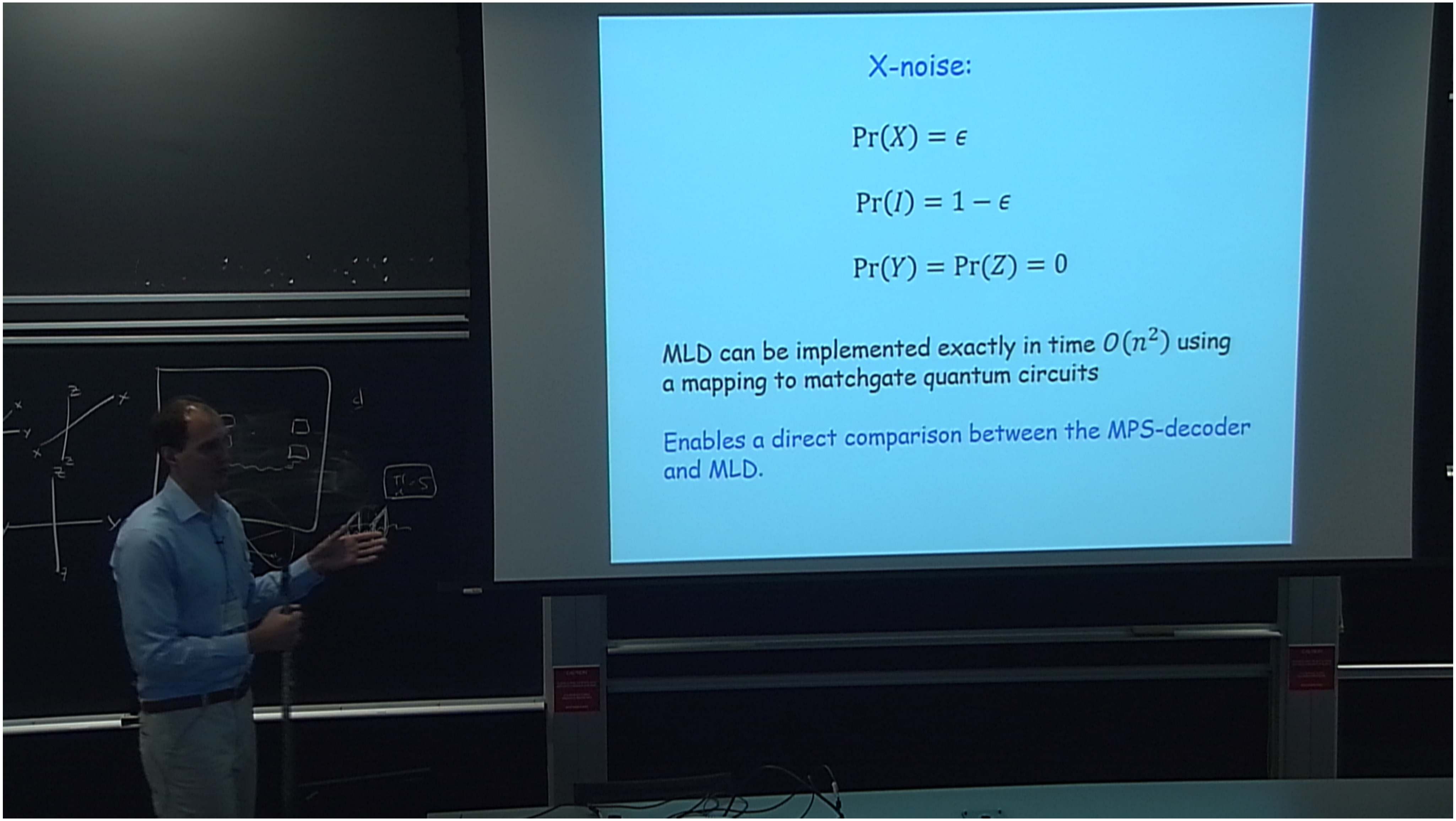

Matrix Product States (MPS)
$\langle i_1 i_2 i_3 i_4 i_5 | \Psi \rangle =$
$A_1(i_1) \cdot A_2(i_2) \cdot A_3(i_3) \cdot A_4(i_4) \cdot A_5(i_5)$

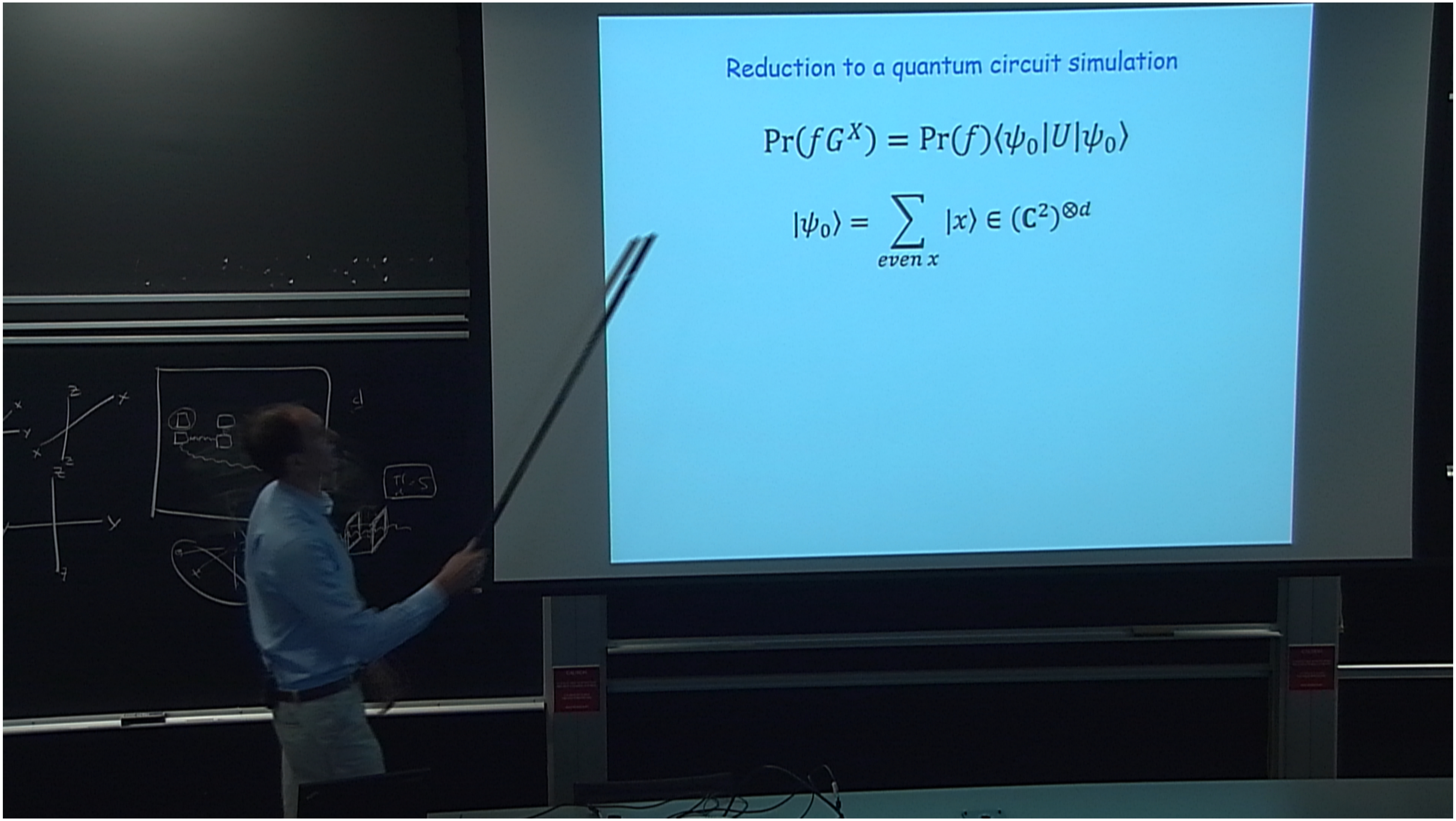

MPS compression
MPS(N, 2χ)
MPS(N, χ)
Ψ
Φ
Efficient compression algorithm:
Schollwock, Ann. Phys. 326, 96 (2011)

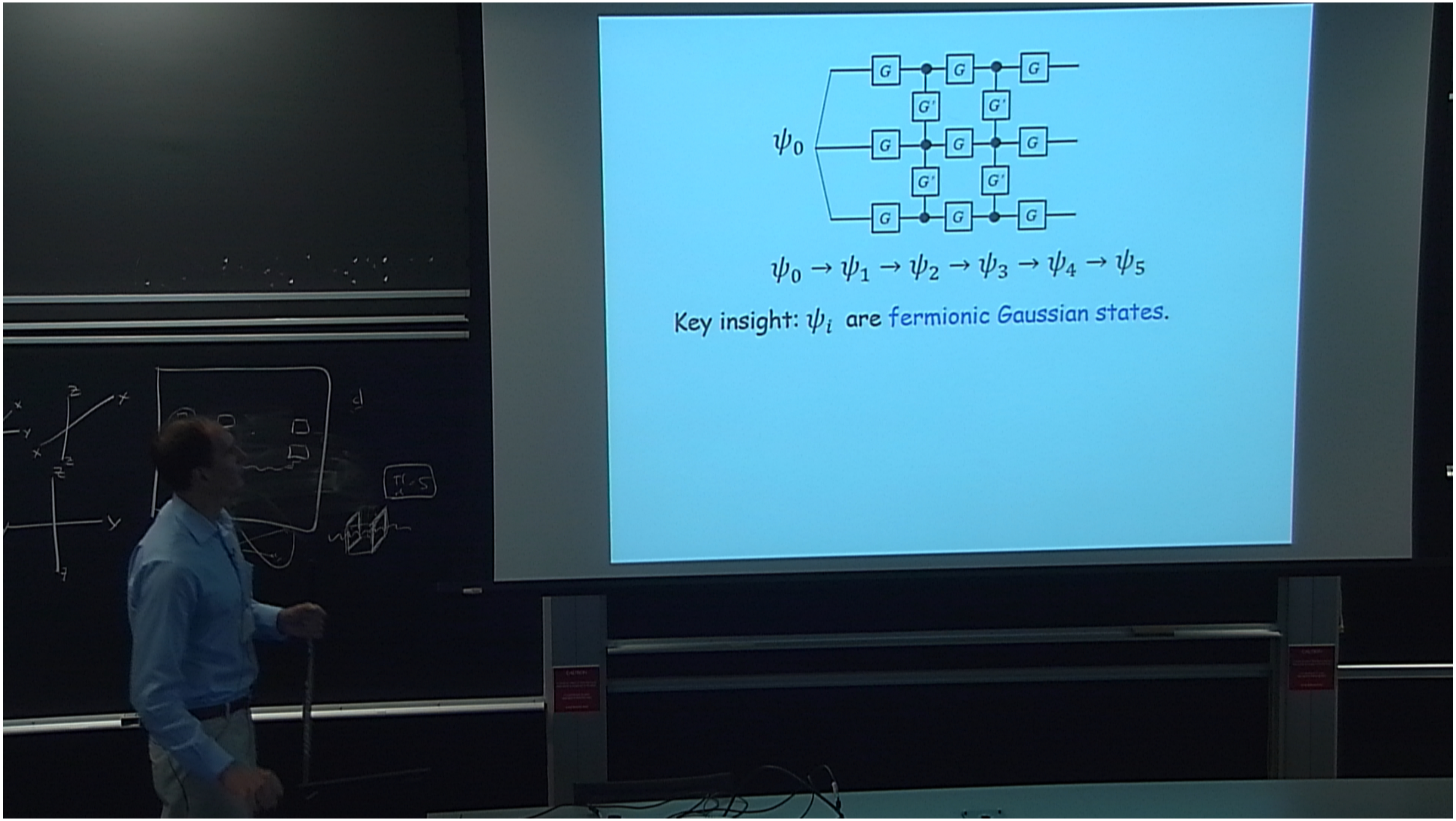

Comparison between MPS and MWM decoders
Depolarizing noise, distance d=25
Logical error probability
Error rate (%)
min matching
MPS, χ=2
MPS, χ=4
MPS, χ=6
MPS, χ=8
Decoder's badness
Error rate (%)



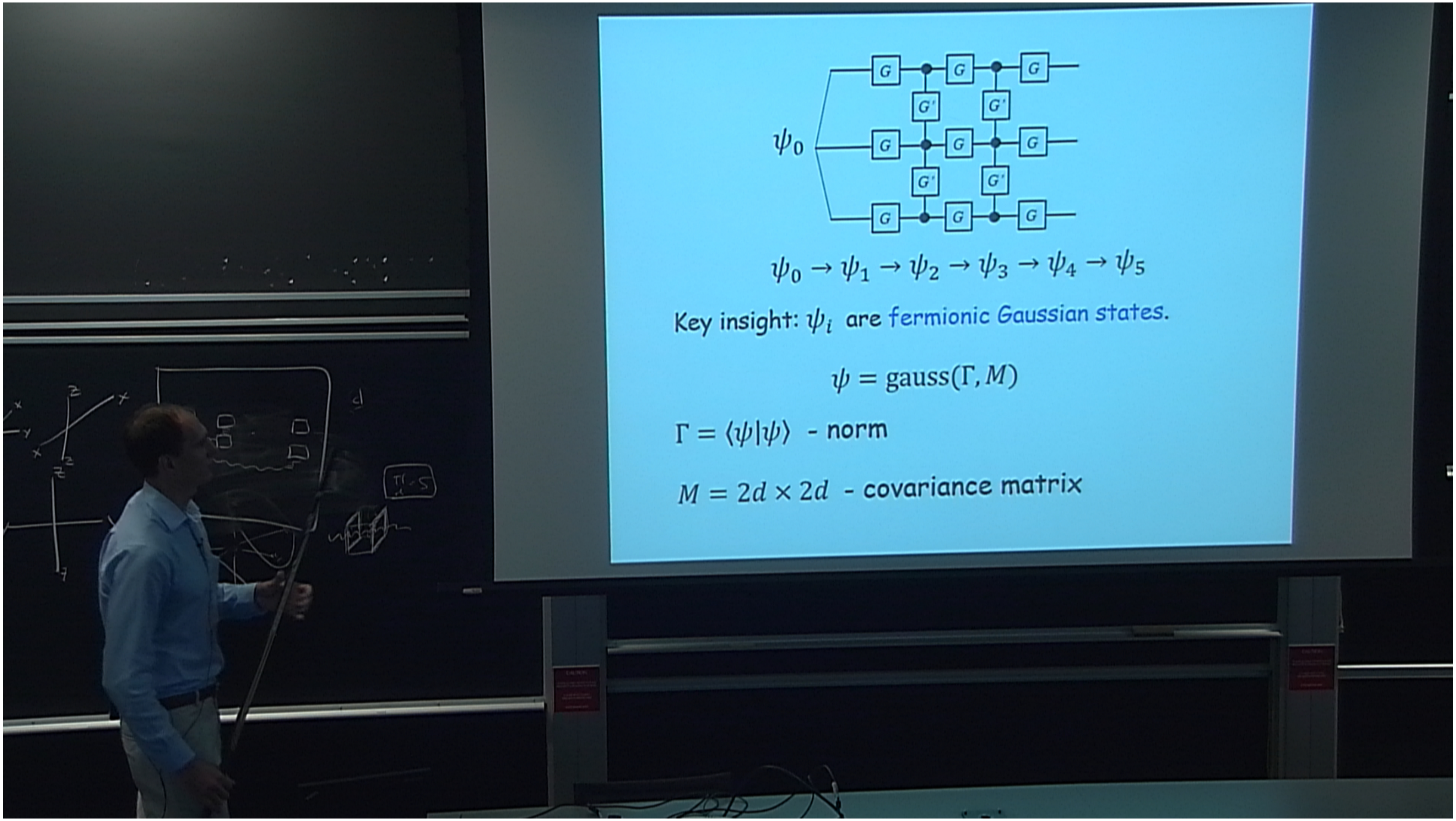
Comparison between MPS and MWM decoders
Depolarizing noise, distance d=25
Logical error probability
Error rate (%)
Decoder's badness
Error rate (%)
min matching
MPS, χ=2
MPS, χ=4
MPS, χ=6
MPS, χ=8


X-noise:
$\Pr(X) = \epsilon$
$\Pr(I) = 1 - \epsilon$
$\Pr(Y) = \Pr(Z) = 0$
MLD can be implemented exactly in time $O(n^2)$ using a mapping to matchgate quantum circuits
Enables a direct comparison between the MPS-decoder and MLD.

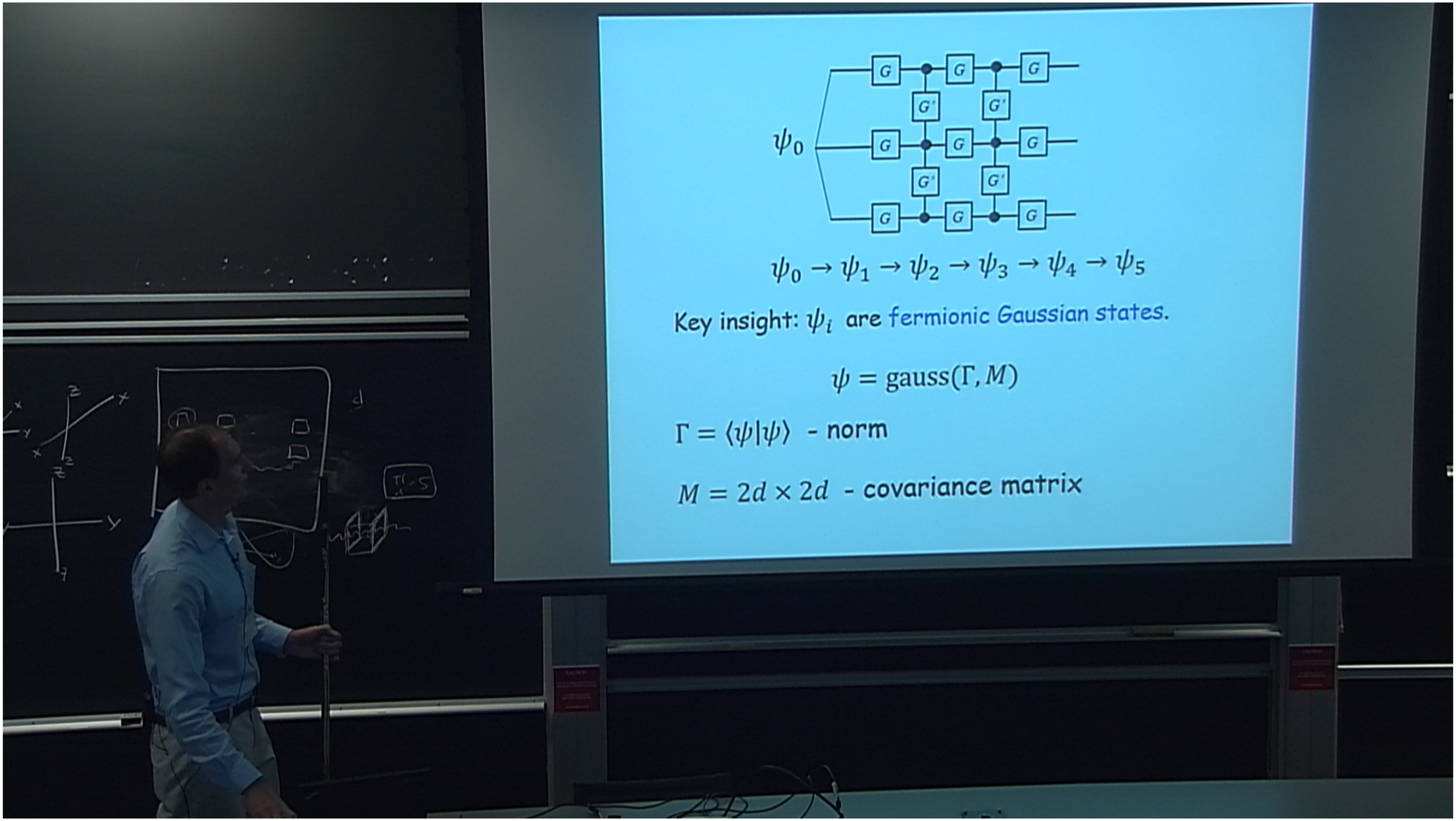

Reduction to a quantum circuit simulation
$\Pr(fG^X) = \Pr(f)\langle\psi_0|U|\psi_0\rangle$
$|\psi_0\rangle = \sum_{even\ x} |x\rangle \in (\mathbb{C}^2)^{\otimes d}$



$\psi_0$
G
G'
$\psi_0 \to \psi_1 \to \psi_2 \to \psi_3 \to \psi_4 \to \psi_5$
Key insight: $\psi_i$ are fermionic Gaussian states.



ψ0
G
G'
ψ0 → ψ1 → ψ2 → ψ3 → ψ4 → ψ5
Key insight: ψi are fermionic Gaussian states.
ψ = gauss(Γ, M)
Γ = ⟨ψ|ψ⟩ - norm
M = 2d × 2d - covariance matrix



$\psi_0$
G
G'
$\psi_0 \to \psi_1 \to \psi_2 \to \psi_3 \to \psi_4 \to \psi_5$
Key insight: $\psi_i$ are fermionic Gaussian states.
$\psi = \mathrm{gauss}(\Gamma, M)$
$\Gamma = \langle\psi|\psi\rangle$ - norm
$M = 2d \times 2d$ - covariance matrix