Title: Applications of the generalized Pauli group in quantum information

Date: Oct 10, 2007 04:00 PM

URL: http://pirsa.org/07100013

Abstract: It is known that finite fields with d elements exist only when d is a prime or a prime power.
When the dimension d of a finite dimensional Hilbert space is a prime power, we can associate to each basis state of the Hilbert space an element of a finite or Galois field, and construct a finite group of unitary transformations, the generalised Pauli group or discrete Heisenberg-Weyl group. Its elements can be expressed, in terms of the elements of a Galois field.
This group presents numerous
applications in Quantum Information Science e.g. tomography, dense coding, teleportation, error correction and so on.
The aim of our talk is to give a general survey of these properties and to present recently obtained results in connection with three problems:
-the so-called "Mean King's problem" in prime power dimension,

-discrete Wigner distributions,

-and quantum tomography .
Finally we shall discuss a limitation of the possible dimensions in which the so-called epistemic interpretation can be consistently formulated, in relation with the existence of finite affine planes, Euler's conjecture and the 36 officers problem.

Applications of the Generalised Pauli Group in Quantum Information.

Dr. Thomas Durt.

Department of Physics, Free University of Brussels,

Pleinlaan 2, 1050 Brussels Belgium;

thomdurt@vub.ac.be

Preliminary remark.

- In many applications of Quantum Information, it happens that different states from a same basis play an identical role.
- Example: Bennett and Brassard protocol for Quantum Key Distribution (B-B'84), two polarisation bases are chosen to encode the signal, and between each of them the two basis states that carry the binary signal (0 and 1) could be intertwined:

  we could permute the values 0 and 1 without changing the essence of the protocol.
- SO it is interesting to consider **groups of permutations of a same basis of the Hilbert space**. Those groups constitue a NATURAL SYMMETRY in many applications that were developed in the framework of Quantum Information.

Example d=2, permutations versus displacement operators in the qubit space.

- Most simple case: two-level systems (QUBITS): d=2.
- Two possible permutations: the identity and the negation (exchange of 0 and 1) which permutes the qubit basis state $|0\rangle$ with $|1\rangle$.
- We can express the identity by the identity operator $|0\rangle\langle 0| + |1\rangle\langle 1|$.
- The operator associated to the negation can be written $|1\rangle\langle 0| + |0\rangle\langle 1|$.
- This operator is equal to the Pauli σ_x operator itself!
- It is diagonal in the basis $(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$.

- We can now repeat the reasoning and consider the two possible permutations of the eigenstates of σ_x.
- We find then the identity operator while the operator that corresponds to the negation is equal to $|0\rangle\langle 0| - |1\rangle\langle 1|$.
- This operator is the Pauli operator σ_z!
- The composition of the operators σ_z et σ_x is equal, up to a global phase, to σ_y.
- σ_y is diagonal in the basis $(\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle))$.
- We find so the 4 Pauli operators:, the identity and the 3 σ (Pauli) operators.

Useful properties of the

Pauli displacement operators (1).

- Such operators form a group (up to global phases), the Pauli group. This group itself consists of 3 commuting subgroups which consist of the identity and one of the 3 operators $\sigma_{x,y,z}$.
- These 3 subgroups are diagonal in the bases:
  $(|0\rangle, |1\rangle)$
  $(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$
  et $(\frac{1}{\sqrt{2}}(|0\rangle + i.|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle))$.
- Such bases are said to be "mutually unbiased" (MUB's):

  Definition: "A collection of orthonormal bases of a d dimensional Hilbert space is said to be mutually unbiased if whenever we choose two states from different bases, the modulus squared of their in-product is equal to $1/d$. "

- The transition probabilities between states from different MUB's are all equal to $1/d$ (in the qubit case they are 50-50 probabilities as when we toss an UNBIASED COIN).

Useful properties of the

Pauli displacement operators (2).

The Pauli operators are in one-to-one correspondence with the so-called Bell states:

$\sigma_0 = |0\rangle\langle 0| + |1\rangle\langle 1| \leftrightarrow |B\rangle_{00} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$

$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| \leftrightarrow |B\rangle_{10} = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$

$\sigma_y = i(|0\rangle\langle 1| - |1\rangle\langle 0|) \leftrightarrow |B\rangle_{11} = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$

$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \leftrightarrow |B\rangle_{01} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$

The Bell states possess plenty of applications in Quantum Information (teleportation, cloning). They are maximally ENTANGLED, maximally NON-LOCAL and form an orthonormal basis of the two-qubit Hilbert space ($d = 4$).

Useful properties of the Pauli displacement operators (3).

- Pauli operators as well as the Bell states form an orthonormal basis of a $d = 4$ Hilbert space.

  Actually, the Pauli displacement operators form an orthonormalised basis of the linear 2x2 operators (relatively to the Trace-norm product).

- As a consequence, any qubit DENSITY MATRIX or density operator is a linear combination of Pauli operators:

  $\rho = \frac{1}{2}(\sigma_0 + k_x\sigma_x + k_y\sigma_y + k_z\sigma_z)$.

  We recognize here Bloch parameters (NMR) or Stokes-Poincaré parameters (polarimetry).

- In order to estimate these parameters it is enough to measure the transition probabilities in the 3 corresponding bases (MUBs).

- By doing so we realize a QUANTUM TOMOGRAPHIC PROCESS so to say we can estimate the qubit quantum state.

Remarks.

- The tomographic procedure based on MUB's is OPTIMAL because there is NO REDUNDANCY between data collected in different bases;

  the information is thus never wasted during the data acquisition.

- The MUB's play an important role in quantum cryptography because they maximize the uncertainty relations: whenever a spy measures the signal on a basis that is mutually unbiased with the basis of encryption, his Shannon information about the signal is equal to zero, so that he does not learn anything about the secret key.

  Therefore encryption bases are often MUB's (examples: BB'84 or 6 states qubit protocols for Quantum Key Distribution).

  In the 6 states protocol for instance the authorized users of the cryptographic channel (Alice and Bob) are able to realize a full tomography of the quantum state that they share, which maximizes the constraints to be met by the spy in order to dissimulate the fact that he eavesdrops the signal. The security of the full protocol (for a given signal to noise ratio) is thus maximal.

Remarks.

- The tomographic procedure based on MUB's is OPTIMAL because there is NO REDUNDANCY between data collected in different bases;

  the information is thus never wasted during the data acquisition.

- The MUB's play an important role in quantum cryptography because they maximize the uncertainty relations: whenever a spy measures the signal on a basis that is mutually unbiased with the basis of encryption, his Shannon information about the signal is equal to zero, so that he does not learn anything about the secret key.

  Therefore encryption bases are often MUB's (examples: BB'84 or 6 states qubit protocols for Quantum Key Distribution).

  In the 6 states protocol for instance the authorized users of the cryptographic channel (Alice and Bob) are able to realize a full tomography of the quantum state that they share, which maximizes the constraints to be met by the spy in order to dissimulate the fact that he eavesdrops the signal. The security of the full protocol (for a given signal to noise ratio) is thus maximal.

Remarks.

- The tomographic procedure based on MUB's is OPTIMAL because there is NO REDUNDANCY between data collected in different bases;

  the information is thus never wasted during the data acquisition.

- The MUB's play an important role in quantum cryptography because they maximize the uncertainty relations: whenever a spy measures the signal on a basis that is mutually unbiased with the basis of encryption, his Shannon information about the signal is equal to zero, so that he does not learn anything about the secret key.

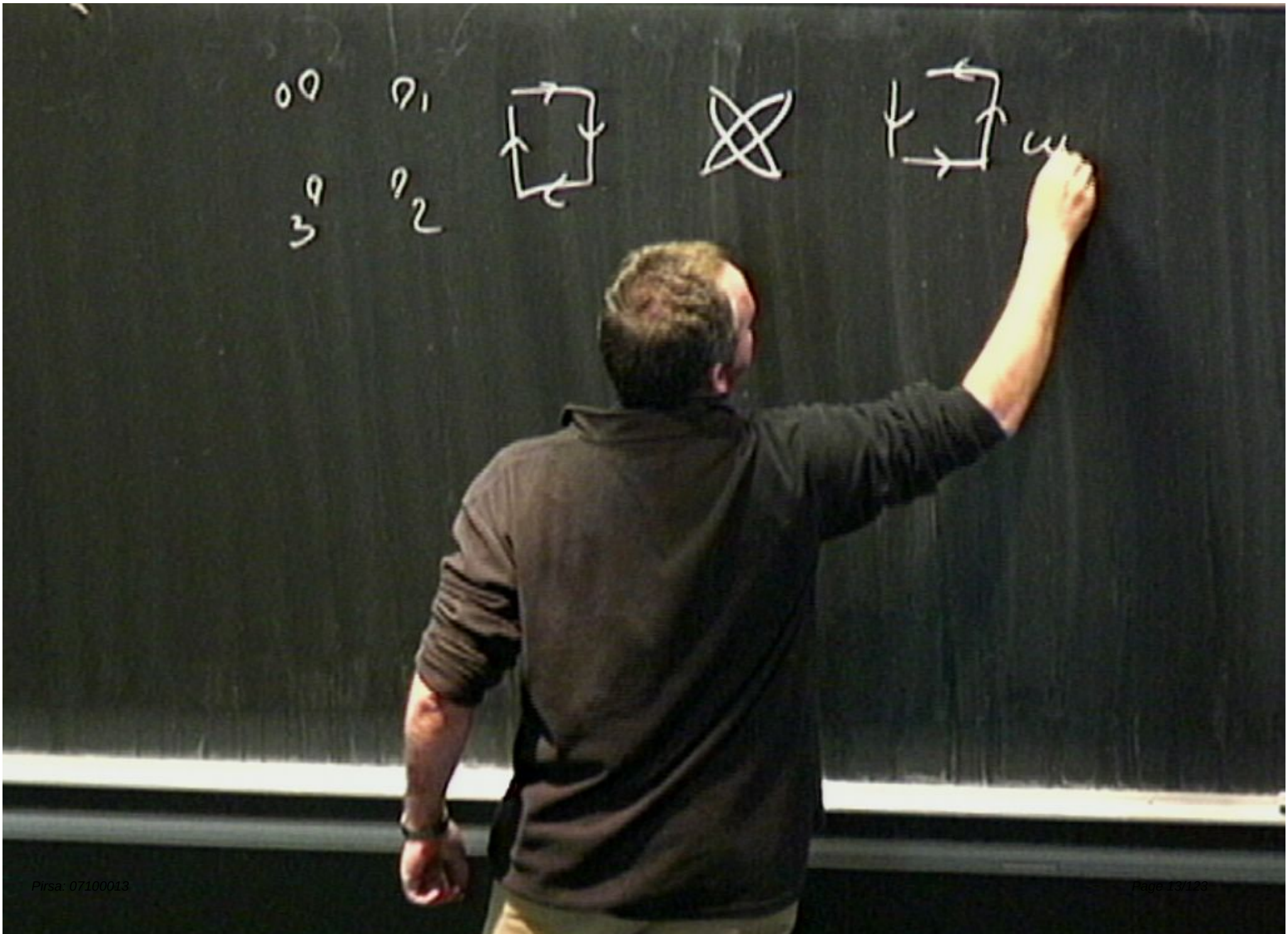
  Therefore encryption bases are often MUB's (examples: BB'84 or 6 states qubit protocols for Quantum Key Distribution).

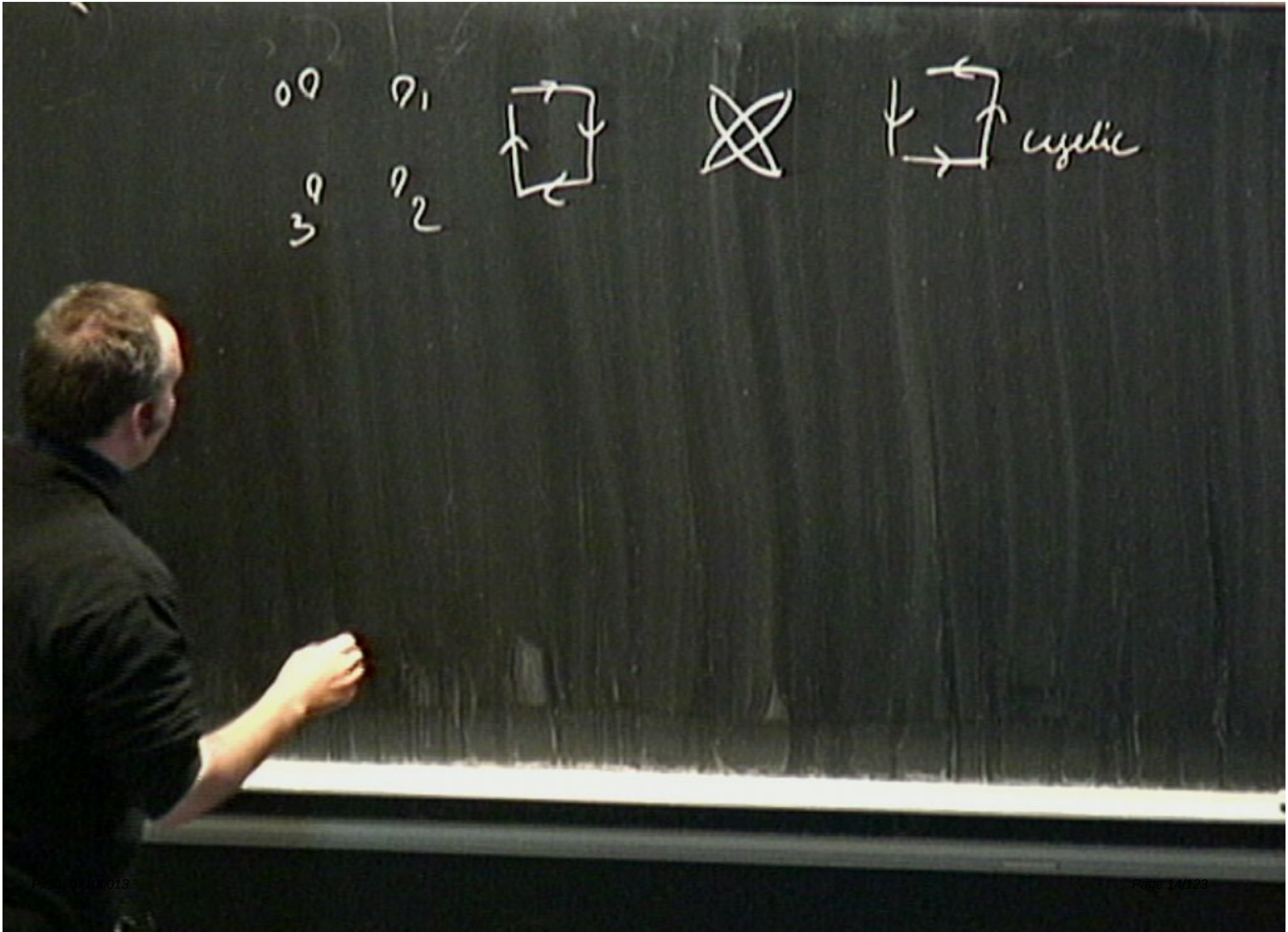
  In the 6 states protocol for instance the authorized users of the cryptographic channel (Alice and Bob) are able to realize a full tomography of the quantum state that they share, which maximizes the constraints to be met by the spy in order to dissimulate the fact that he eavesdrops the signal. The security of the full protocol (for a given signal to noise ratio) is thus maximal.

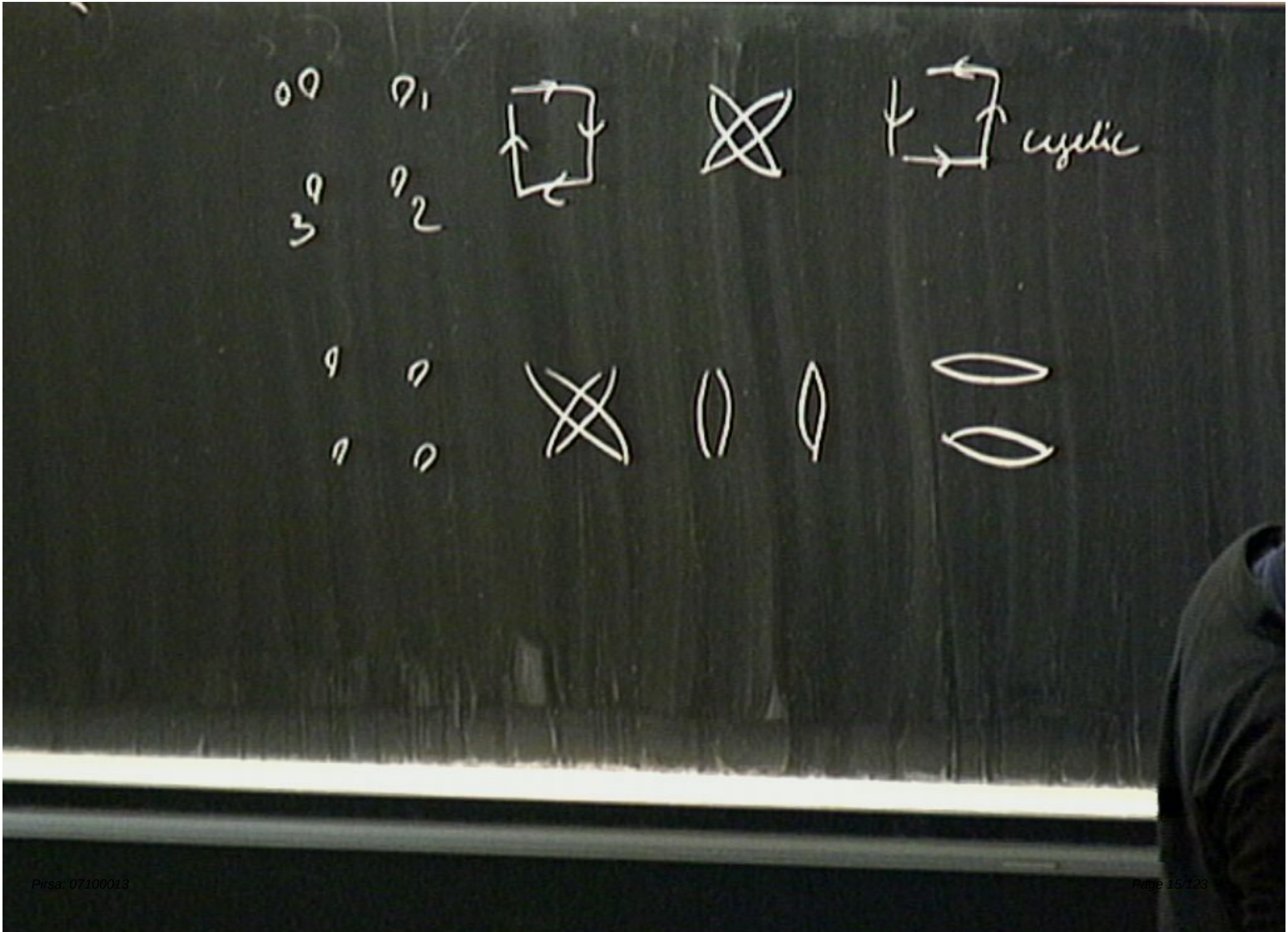
Generalisations in dimensions higher than 2.

Dimension 4.

- There exist, in dimension 4, 4.3.2=24 permutations between states from a same basis. Two subgroups of this group of 24 elements are particularly interesting:
- The cyclic group with 4 elements generated by the permutation
  $P_1 = |0\rangle \rightarrow |1\rangle;|1\rangle \rightarrow |2\rangle;|2\rangle \rightarrow |3\rangle;|3\rangle \rightarrow |4\rangle.$
  It also contains the identity P_0, and the powers 2 and 3 of the generator:
  $P_2 = |0\rangle \rightarrow |2\rangle;|1\rangle \rightarrow |3\rangle;|2\rangle \rightarrow |0\rangle;|3\rangle \rightarrow |1\rangle.$
  $P_3 = |0\rangle \rightarrow |3\rangle;|1\rangle \rightarrow |0\rangle;|2\rangle \rightarrow |1\rangle;|3\rangle \rightarrow |2\rangle.$
- The "Galois" group that contains the identity and the 3 following permutations:
  $P'_1 = |0\rangle \rightarrow |1\rangle;|1\rangle \rightarrow |0\rangle;|2\rangle \rightarrow |3\rangle;|3\rangle \rightarrow |2\rangle.$
  $P'_2 = |0\rangle \rightarrow |2\rangle;|1\rangle \rightarrow |3\rangle;|2\rangle \rightarrow |0\rangle;|3\rangle \rightarrow |1\rangle.$
  $P'_3 = |0\rangle \rightarrow |3\rangle;|1\rangle \rightarrow |2\rangle;|2\rangle \rightarrow |1\rangle;|3\rangle \rightarrow |0\rangle.$


00
η1
η2


00
η_1
3^9
η_2
cyclic


cyclic

On the basis of the composition law of these (commutative) groups it is easy to define a (commutative) addition law through the relation
$P_i.P_j = P_{i+j}\ (i, j = 0, 1, 2, 3)$.
We find so the following addition tables:

$+_{cycl.}$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	2	3	0
2.	2	3	0	1
3.	3	0	1	2

(1)

$\oplus_G$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	0	3	2
2.	2	3	0	1
3.	3	2	1	0

(2)

Such algebraic structures are called "COMMUTATIVE RINGS"; the Galois multiplication is endowed with a remarkable property:
THERE IS NO DIVIDER OF ZERO, EXCEPTED ZERO ITSELF...
Therefore the Galois ring is also called a FIELD (finite field).
Finite fields were studied by Evariste Galois in the 19th century.
On the basis of such operations we can now define generalised Pauli operators: those operators form a finite displacement group, the generalised Pauli or Heisenberg-Weyl group which constitutes a discrete version of the continuous phase-space displacement operators (largely used in quantum optics).
Such operators are unitary and can be defined as follows (T. Durt: "A new expression for mutually unbiased bases in prime power dimensions", J. Phys. A: Math. Gen. 38 (2005) 5267-5283):

$$V_i^j = \sum_{k=0}^{d-1} \gamma_G^{((k \oplus_G i) \odot_G j)} |k \oplus_G i\rangle\langle k|, \qquad (5)$$

where $\oplus_G$ and $\odot_G$ represent the operations (addition and multiplication) of the finite field while γ_G is a well-chosen phase (pth root of unity: $\gamma_G = e^{i.2\pi/p}$). **This construction works in PRIME and PRIME POWER DIMENSIONS ONLY. Whenever the dimension is prime, these operations reduce to modulo d (p) operations.**

Such algebraic structures are called "COMMUTATIVE RINGS"; the Galois multiplication is endowed with a remarkable property:
THERE IS NO DIVIDER OF ZERO, EXCEPTED ZERO ITSELF...
Therefore the Galois ring is also called a FIELD (finite field).
Finite fields were studied by Evariste Galois in the 19th century.
On the basis of such operations we can now define generalised Pauli operators: those operators form a finite displacement group, the generalised Pauli or Heisenberg-Weyl group which constitutes a discrete version of the continuous phase-space displacement operators (largely used in quantum optics).
Such operators are unitary and can be defined as follows (T. Durt: "A new expression for mutually unbiased bases in prime power dimensions", J. Phys. A: Math. Gen. 38 (2005) 5267-5283):

$$V_i^j = \sum_{k=0}^{d-1} \gamma_G^{((k \oplus_G i) \odot_G j)} |k \oplus_G i\rangle\langle k|, \qquad (5)$$

where $\oplus_G$ and $\odot_G$ represent the operations (addition and multiplication) of the finite field while γ_G is a well-chosen phase (pth root of unity: $\gamma_G = e^{i.2\pi/p}$). **This construction works in PRIME and PRIME POWER DIMENSIONS ONLY. Whenever the dimension is prime, these operations reduce to modulo d (p) operations.**

On the basis of these addition tables it is also easy to define a (commutative) multiplication law that is distributive relatively to the addition:,
We find so the following multiplication tables:

$\cdot_{cycl.}$	0.	1.	2.	3.
0.	0	0	0	0
1.	0	1	2	3
2.	0	2	0	2
3.	0	3	2	1

(3)

Remark:
The addition and the "cyclic" multiplication are nothing else than the MODULO 4 addition and multiplication.

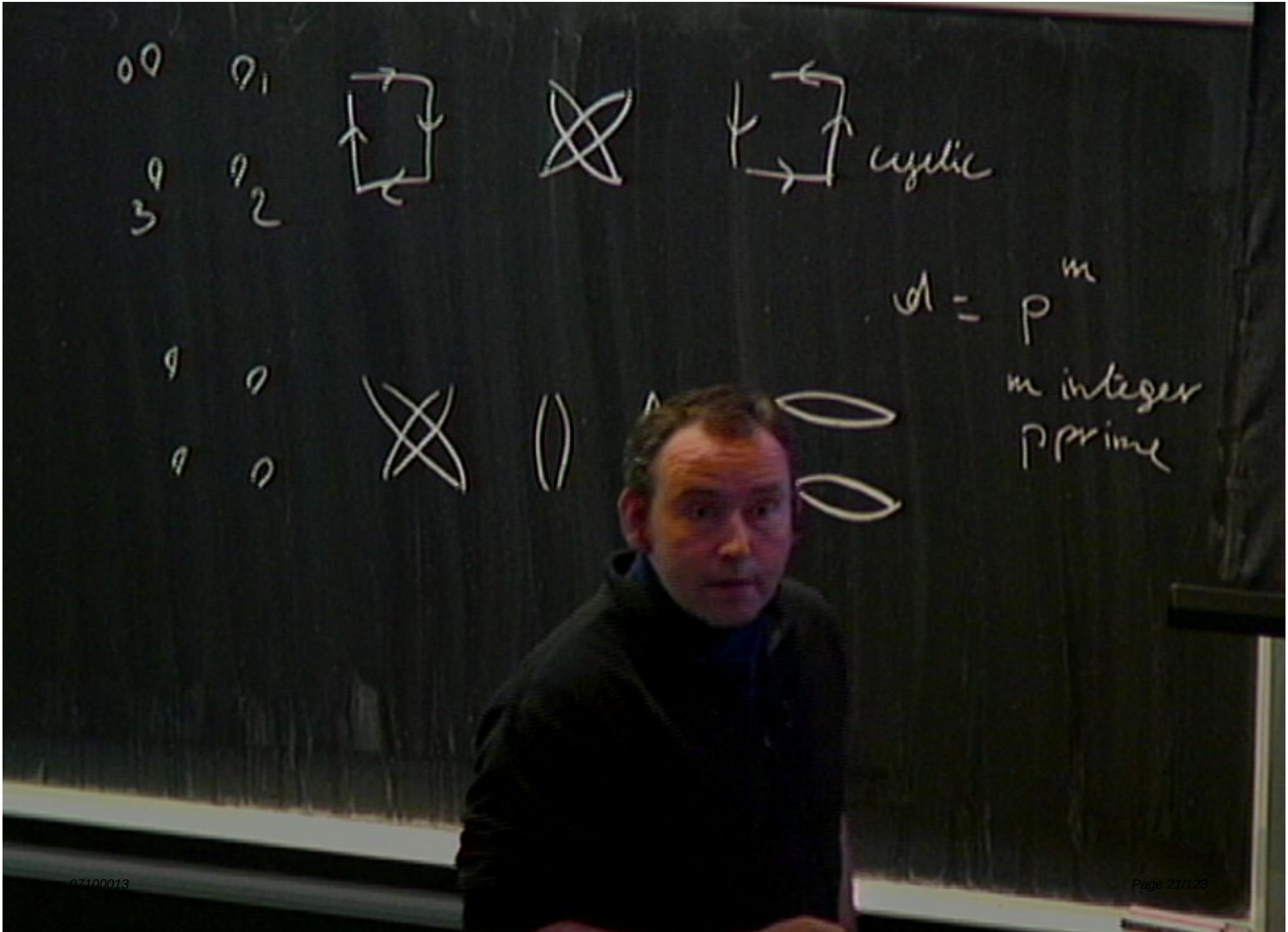
$\odot_G$	0.	1.	2.	3.
0.	0	0	0	0
1.	0	1	2	3
2.	0	2	3	1
3.	0	3	1	2

(4)

Such algebraic structures are called "COMMUTATIVE RINGS"; the Galois multiplication is endowed with a remarkable property:
THERE IS NO DIVIDER OF ZERO, EXCEPTED ZERO ITSELF...
Therefore the Galois ring is also called a FIELD (finite field).
Finite fields were studied by Evariste Galois in the 19th century.
On the basis of such operations we can now define generalised Pauli operators: those operators form a finite displacement group, the generalised Pauli or Heisenberg-Weyl group which constitutes a discrete version of the continuous phase-space displacement operators (largely used in quantum optics).
Such operators are unitary and can be defined as follows (T. Durt: "A new expression for mutually unbiased bases in prime power dimensions", J. Phys. A: Math. Gen. 38 (2005) 5267-5283):

$$V_i^j = \sum_{k=0}^{d-1} \gamma_G^{((k \oplus_G i) \odot_G j)} |k \oplus_G i\rangle\langle k|, \qquad (5)$$

where $\oplus_G$ and $\odot_G$ represent the operations (addition and multiplication) of the finite field while γ_G is a well-chosen phase (pth root of unity: $\gamma_G = e^{i.2\pi/p}$). **This construction works in PRIME and PRIME POWER DIMENSIONS ONLY. Whenever the dimension is prime, these operations reduce to modulo d (p) operations.**


cyclic
$d = p^m$
m integer
p prime

On the basis of the composition law of these (commutative) groups it is easy to define a (commutative) addition law through the relation
$P_i.P_j = P_{i+j}\ (i, j = 0, 1, 2, 3)$.
We find so the following addition tables:

$+_{cycl.}$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	2	3	0
2.	2	3	0	1
3.	3	0	1	2

(1)

$\oplus_G$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	0	3	2
2.	2	3	0	1
3.	3	2	1	0

(2)

On the basis of the composition law of these (commutative) groups it is easy to define a (commutative) addition law through the relation
$P_i.P_j = P_{i+j}\ (i,j = 0,1,2,3)$.
We find so the following addition tables:

$+_{cycl.}$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	2	3	0
2.	2	3	0	1
3.	3	0	1	2

(1)

$\oplus_G$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	0	3	2
2.	2	3	0	1
3.	3	2	1	0

(2)

On the basis of the composition law of these (commutative) groups it is easy to define a (commutative) addition law through the relation
$P_i.P_j = P_{i+j}\ (i, j = 0, 1, 2, 3)$.
We find so the following addition tables:

$+_{cycl.}$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	2	3	0
2.	2	3	0	1
3.	3	0	1	2

(1)

$\oplus_G$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	0	3	2
2.	2	3	0	1
3.	3	2	1	0

(2)

On the basis of these addition tables it is also easy to define a (commutative) multiplication law that is distributive relatively to the addition:,
We find so the following multiplication tables:

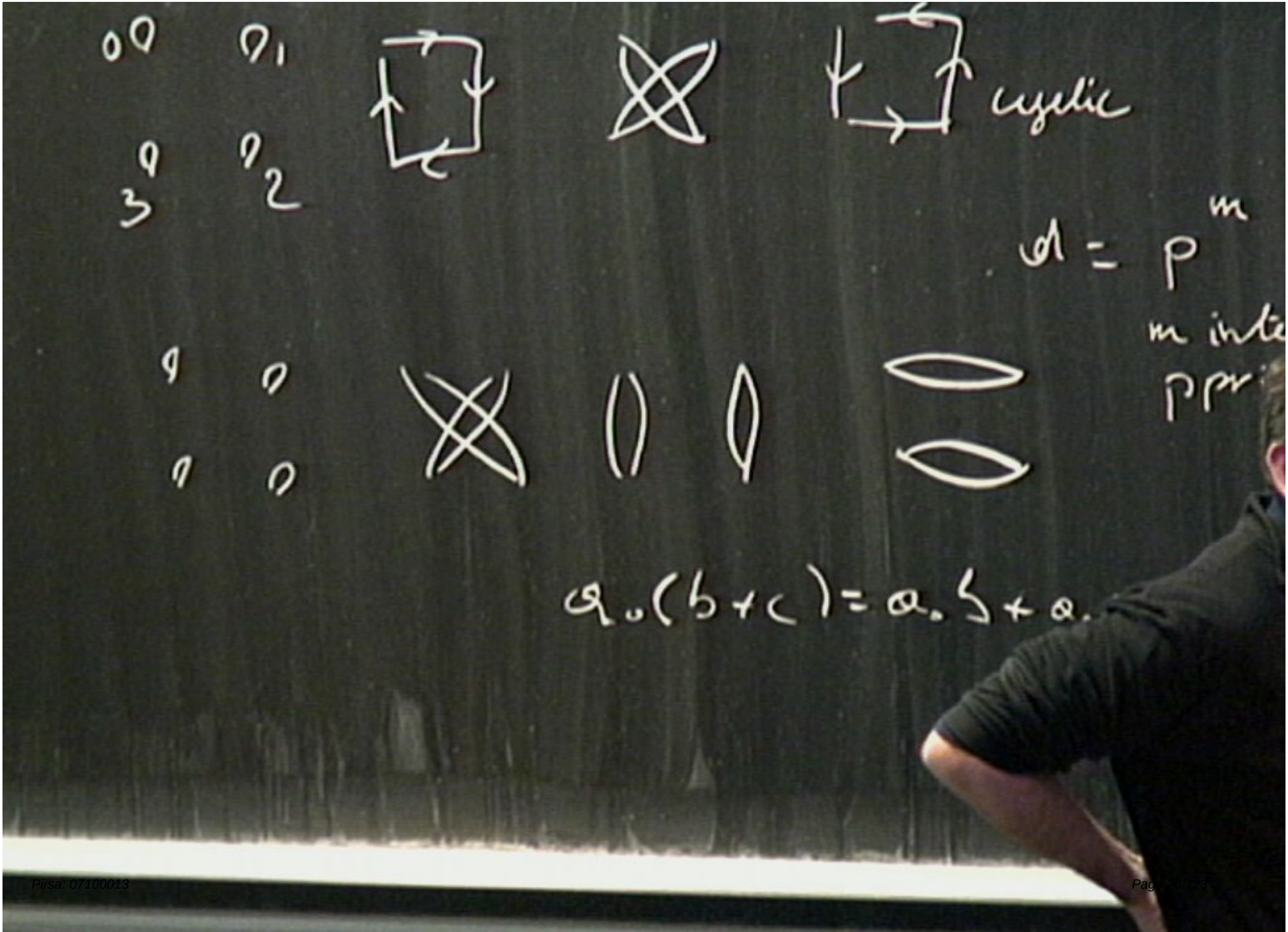
$\cdot_{cycl.}\cdot$	0.	1.	2.	3.
0.	0	0	0	0
1.	0	1	2	3
2.	0	2	0	2
3.	0	3	2	1

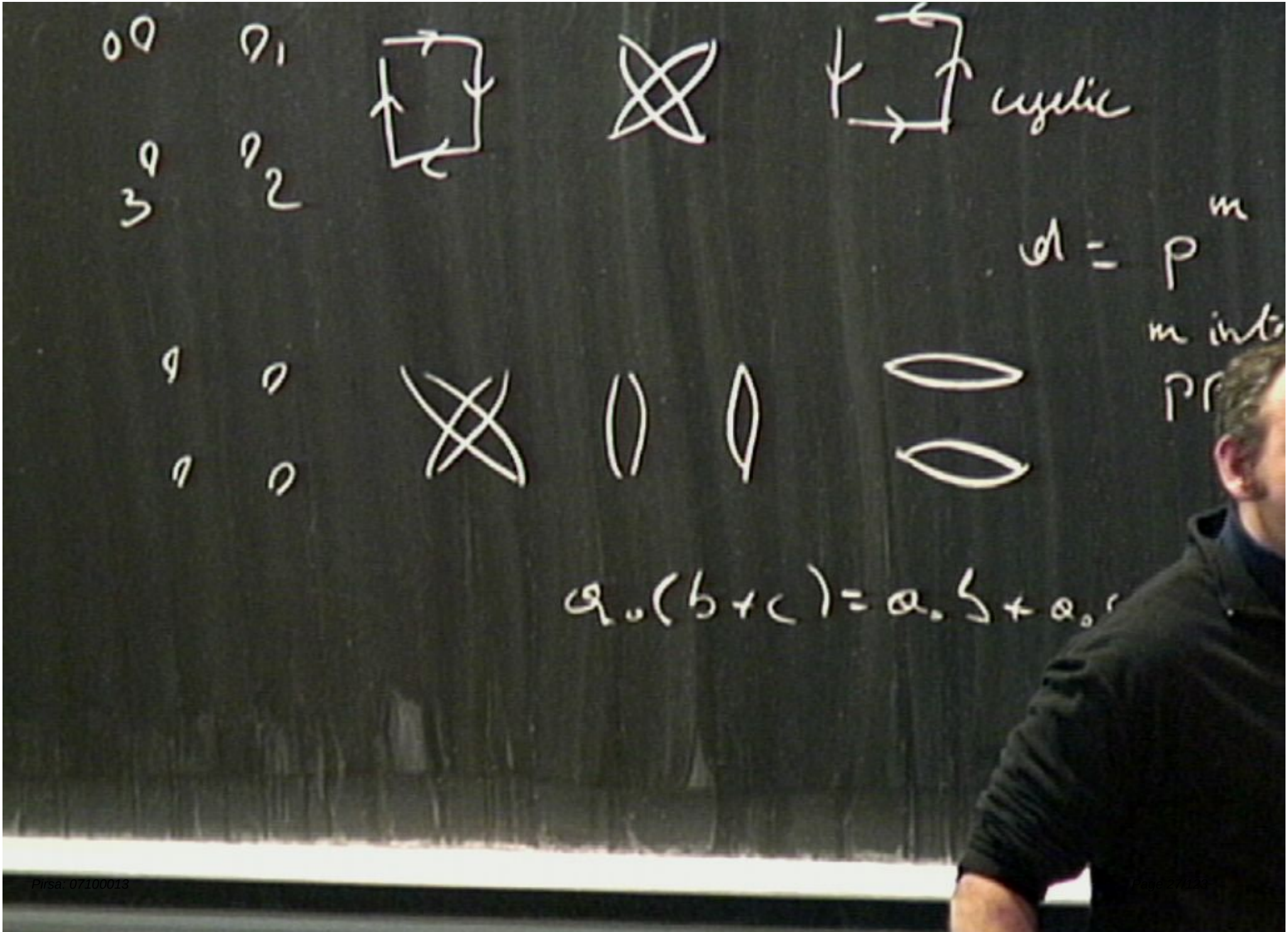
(3)

Remark:
The addition and the "cyclic" multiplication are nothing else than the MOD-ULO 4 addition and multiplication.

$\odot_G\cdot$	0.	1.	2.	3.
0.	0	0	0	0
1.	0	1	2	3
2.	0	2	3	1
3.	0	3	1	2

(4)

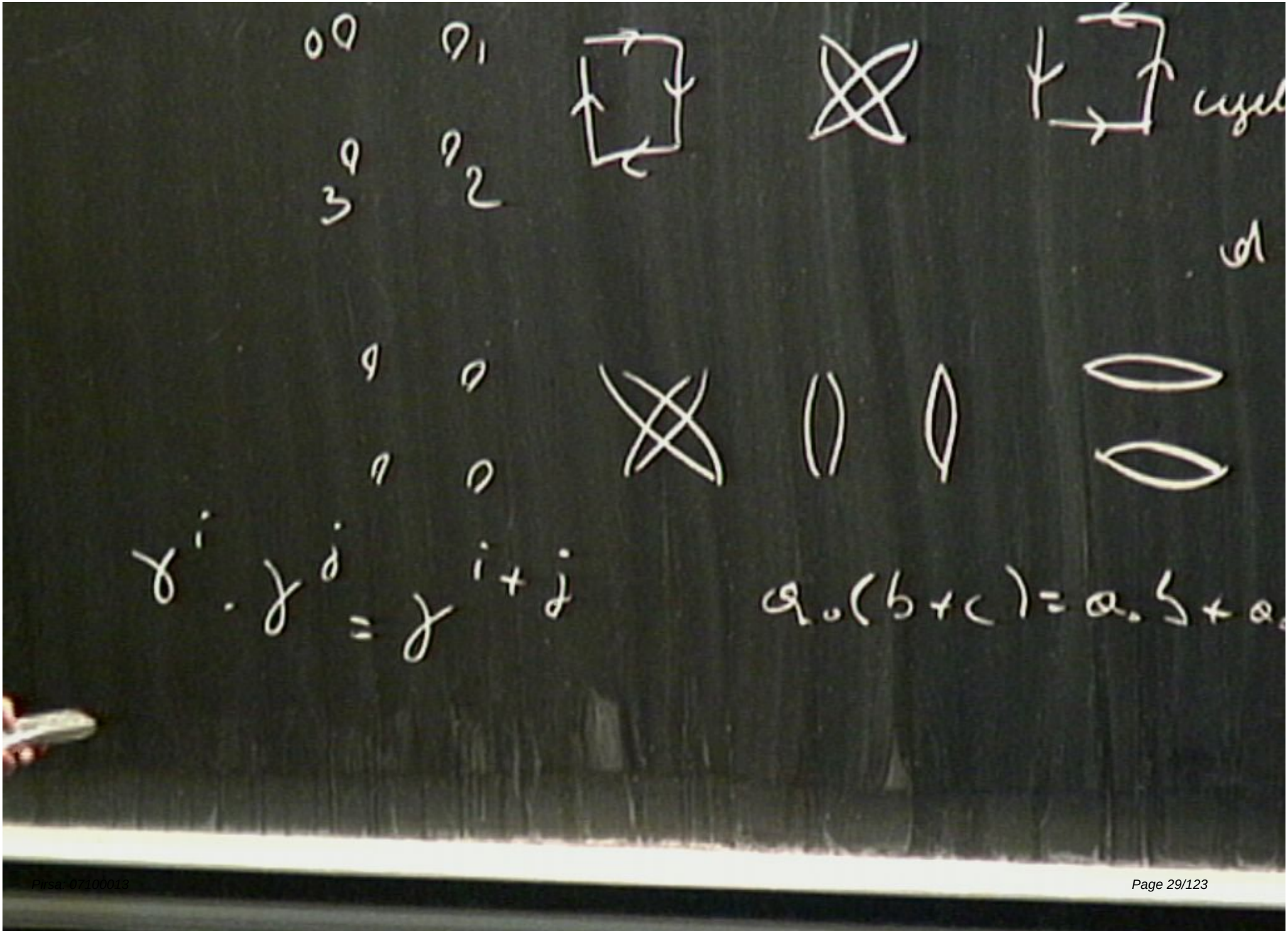

cyclic
$d = p^m$
m inte
ppri
$a \cdot (b + c) = a \cdot b + a \cdot$



Such algebraic structures are called "COMMUTATIVE RINGS"; the Galois multiplication is endowed with a remarkable property:
THERE IS NO DIVIDER OF ZERO, EXCEPTED ZERO ITSELF...
Therefore the Galois ring is also called a FIELD (finite field).
Finite fields were studied by Evariste Galois in the 19th century.
On the basis of such operations we can now define generalised Pauli operators: those operators form a finite displacement group, the generalised Pauli or Heisenberg-Weyl group which constitutes a discrete version of the continuous phase-space displacement operators (largely used in quantum optics).
Such operators are unitary and can be defined as follows (T. Durt: "A new expression for mutually unbiased bases in prime power dimensions", J. Phys. A: Math. Gen. 38 (2005) 5267-5283):

$$V_i^j = \sum_{k=0}^{d-1} \gamma_G^{((k \oplus_G i) \odot_G j)} |k \oplus_G i\rangle\langle k|, \qquad (5)$$

where $\oplus_G$ and $\odot_G$ represent the operations (addition and multiplication) of the finite field while γ_G is a well-chosen phase (pth root of unity: $\gamma_G = e^{i.2\pi/p}$). **This construction works in PRIME and PRIME POWER DIMENSIONS ONLY. Whenever the dimension is prime, these operations reduce to modulo d (p) operations.**


$\gamma^i \cdot \gamma^j = \gamma^{i+j}$
$a \cdot (b+c) = a \cdot b + a$

The generalised Pauli group presents numerous applications in Quantum Information (tomograpy, dense coding,teleportation, cloning, error correction and so on). One can show that:

$$\sum_{j=0}^{d-1} \gamma_G^{(j \odot_G i)} = d\delta_{i,0} \tag{6}$$

$$\gamma_G^i \cdot \gamma_G^j = \gamma_G^{(i \oplus_G j)} \tag{7}$$

Besides, the Galois addition factorizes; for instance, in dimension 4, if we express quartits like tensorial products of 2 qubits: $|0\rangle_4 = |0\rangle_2 \otimes |0\rangle_2$, $|1\rangle_4 = |0\rangle_2 \otimes |1\rangle_2$, $|2\rangle_4 = |1\rangle_2 \otimes |0\rangle_2$, $|3\rangle_4 = |1\rangle_2 \otimes |1\rangle_2$,we can check at the level of the addition table that
if $|i\rangle_4 = |i_1\rangle_2 \otimes |i_2\rangle_2$, et $|j\rangle_4 = |j_1\rangle_2 \otimes |j_2\rangle_2$,
then $|i \oplus_G j\rangle_4 = |i_1 \oplus_{mod2} j_1\rangle_2 \otimes |i_2 \oplus_{mod2} j_2\rangle_2$.
This means that the (quartit here) addition FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE. In dimension p^m, with p prime and m a positive integer the Galois addition always FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE.
The Galois multiplication table is more involved but the corresponding tables are well known and are available, for instance on the web.

The generalised Pauli group presents numerous applications in Quantum Information (tomograpy, dense coding,teleportation, cloning, error correction and so on). One can show that:

$$\sum_{j=0}^{d-1} \gamma_G^{(j \odot_G i)} = d\delta_{i,0} \tag{6}$$

$$\gamma_G^i \cdot \gamma_G^j = \gamma_G^{(i \oplus_G j)} \tag{7}$$

Besides, the Galois addition factorizes; for instance, in dimension 4, if we express quartits like tensorial products of 2 qubits: $|0\rangle_4 = |0\rangle_2 \otimes |0\rangle_2$, $|1\rangle_4 = |0\rangle_2 \otimes |1\rangle_2$, $|2\rangle_4 = |1\rangle_2 \otimes |0\rangle_2$, $|3\rangle_4 = |1\rangle_2 \otimes |1\rangle_2$,we can check at the level of the addition table that
if $|i\rangle_4 = |i_1\rangle_2 \otimes |i_2\rangle_2$, et $|j\rangle_4 = |j_1\rangle_2 \otimes |j_2\rangle_2$,
then $|i \oplus_G j\rangle_4 = |i_1 \oplus_{mod2} j_1\rangle_2 \otimes |i_2 \oplus_{mod2} j_2\rangle_2$.
This means that the (quartit here) addition FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE. In dimension p^m, with p prime and m a positive integer the Galois addition always FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE.
The Galois multiplication table is more involved but the corresponding tables are well known and are available, for instance on the web.

The generalised Pauli group presents numerous applications in Quantum Information (tomograpy, dense coding,teleportation, cloning, error correction and so on). One can show that:

$$\sum_{j=0}^{d-1} \gamma_G^{(j \odot_G i)} = d\delta_{i,0} \tag{6}$$

$$\gamma_G^i \cdot \gamma_G^j = \gamma_G^{(i \oplus_G j)} \tag{7}$$

Besides, the Galois addition factorizes; for instance, in dimension 4, if we express quartits like tensorial products of 2 qubits: $|0\rangle_4 = |0\rangle_2 \otimes |0\rangle_2$, $|1\rangle_4 = |0\rangle_2 \otimes |1\rangle_2$, $|2\rangle_4 = |1\rangle_2 \otimes |0\rangle_2$, $|3\rangle_4 = |1\rangle_2 \otimes |1\rangle_2$,we can check at the level of the addition table that
if $|i\rangle_4 = |i_1\rangle_2 \otimes |i_2\rangle_2$, et $|j\rangle_4 = |j_1\rangle_2 \otimes |j_2\rangle_2$,
then $|i \oplus_G j\rangle_4 = |i_1 \oplus_{mod2} j_1\rangle_2 \otimes |i_2 \oplus_{mod2} j_2\rangle_2$.
This means that the (quartit here) addition FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE. In dimension p^m, with p prime and m a positive integer the Galois addition always FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE.
The Galois multiplication table is more involved but the corresponding tables are well known and are available, for instance on the web.

On the basis of these addition tables it is also easy to define a (commutative) multiplication law that is distributive relatively to the addition:,
We find so the following multiplication tables:

$\cdot_{cycl.}$	0.	1.	2.	3.
0.	0	0	0	0
1.	0	1	2	3
2.	0	2	0	2
3.	0	3	2	1

(3)

Remark:
The addition and the "cyclic" multiplication are nothing else than the MOD-ULO 4 addition and multiplication.

$\odot_G$	0.	1.	2.	3.
0.	0	0	0	0
1.	0	1	2	3
2.	0	2	3	1
3.	0	3	1	2

(4)

On the basis of the composition law of these (commutative) groups it is easy to define a (commutative) addition law through the relation
$P_i.P_j = P_{i+j}\ (i,j = 0,1,2,3)$.
We find so the following addition tables:

$+_{cycl.}$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	2	3	0
2.	2	3	0	1
3.	3	0	1	2

(1)

$\oplus_G$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	0	3	2
2.	2	3	0	1
3.	3	2	1	0

(2)

On the basis of these addition tables it is also easy to define a (commutative) multiplication law that is distributive relatively to the addition:,
We find so the following multiplication tables:

$\cdot_{cycl.}$	0.	1.	2.	3.
0.	0	0	0	0
1.	0	1	2	3
2.	0	2	0	2
3.	0	3	2	1

(3)

Remark:
The addition and the "cyclic" multiplication are nothing else than the MOD-ULO 4 addition and multiplication.

$\odot_G$	0.	1.	2.	3.
0.	0	0	0	0
1.	0	1	2	3
2.	0	2	3	1
3.	0	3	1	2

(4)

Such algebraic structures are called "COMMUTATIVE RINGS"; the Galois multiplication is endowed with a remarkable property:
THERE IS NO DIVIDER OF ZERO, EXCEPTED ZERO ITSELF...
Therefore the Galois ring is also called a FIELD (finite field).
Finite fields were studied by Evariste Galois in the 19th century.
On the basis of such operations we can now define generalised Pauli operators: those operators form a finite displacement group, the generalised Pauli or Heisenberg-Weyl group which constitutes a discrete version of the continuous phase-space displacement operators (largely used in quantum optics).
Such operators are unitary and can be defined as follows (T. Durt: "A new expression for mutually unbiased bases in prime power dimensions", J. Phys. A: Math. Gen. 38 (2005) 5267-5283):

$$V_i^j = \sum_{k=0}^{d-1} \gamma_G^{((k \oplus_G i) \odot_G j)} |k \oplus_G i\rangle\langle k|, \qquad (5)$$

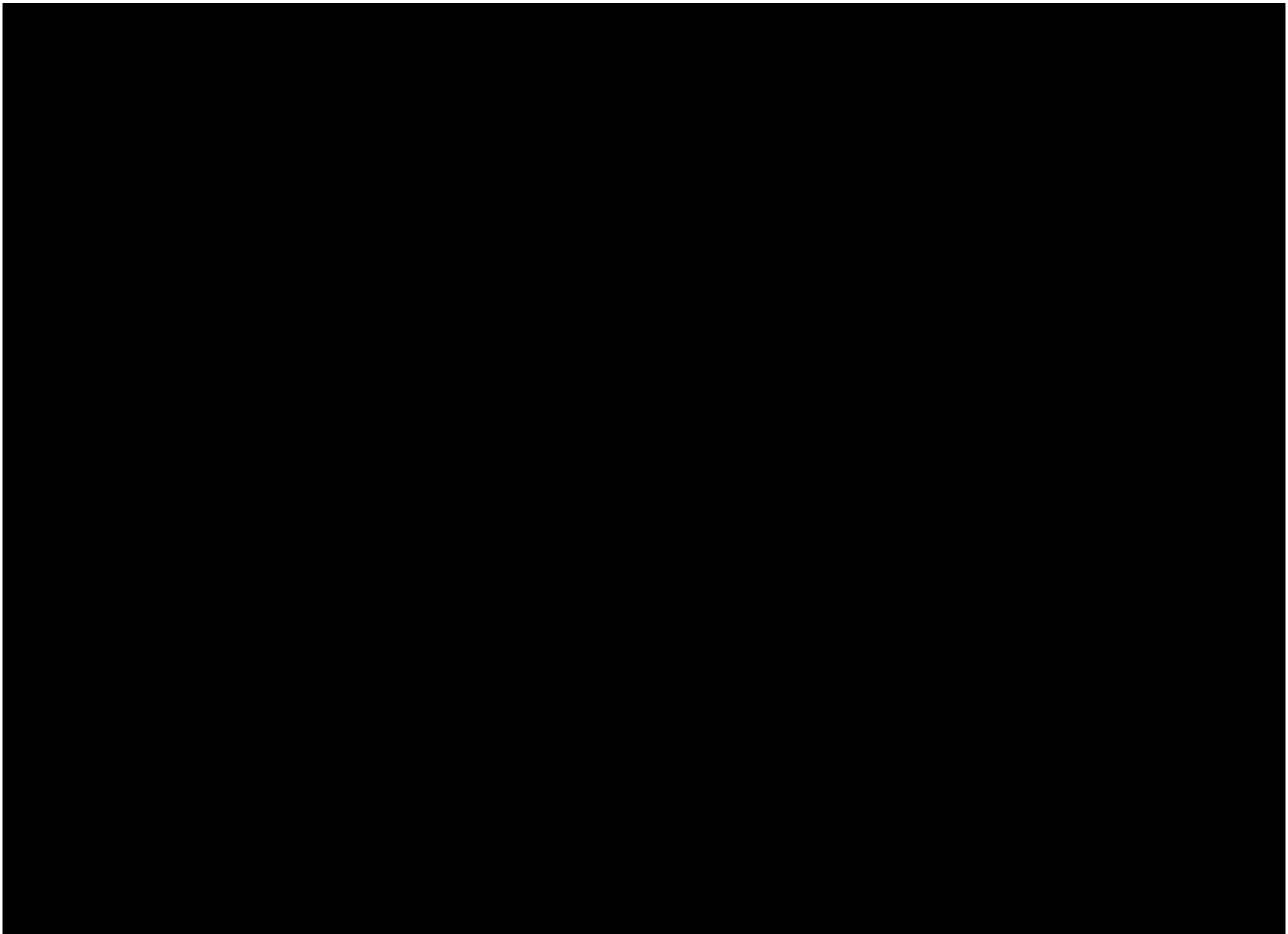
where $\oplus_G$ and $\odot_G$ represent the operations (addition and multiplication) of the finite field while γ_G is a well-chosen phase (pth root of unity: $\gamma_G = e^{i.2\pi/p}$). **This construction works in PRIME and PRIME POWER DIMENSIONS ONLY. Whenever the dimension is prime, these operations reduce to modulo d (p) operations.**

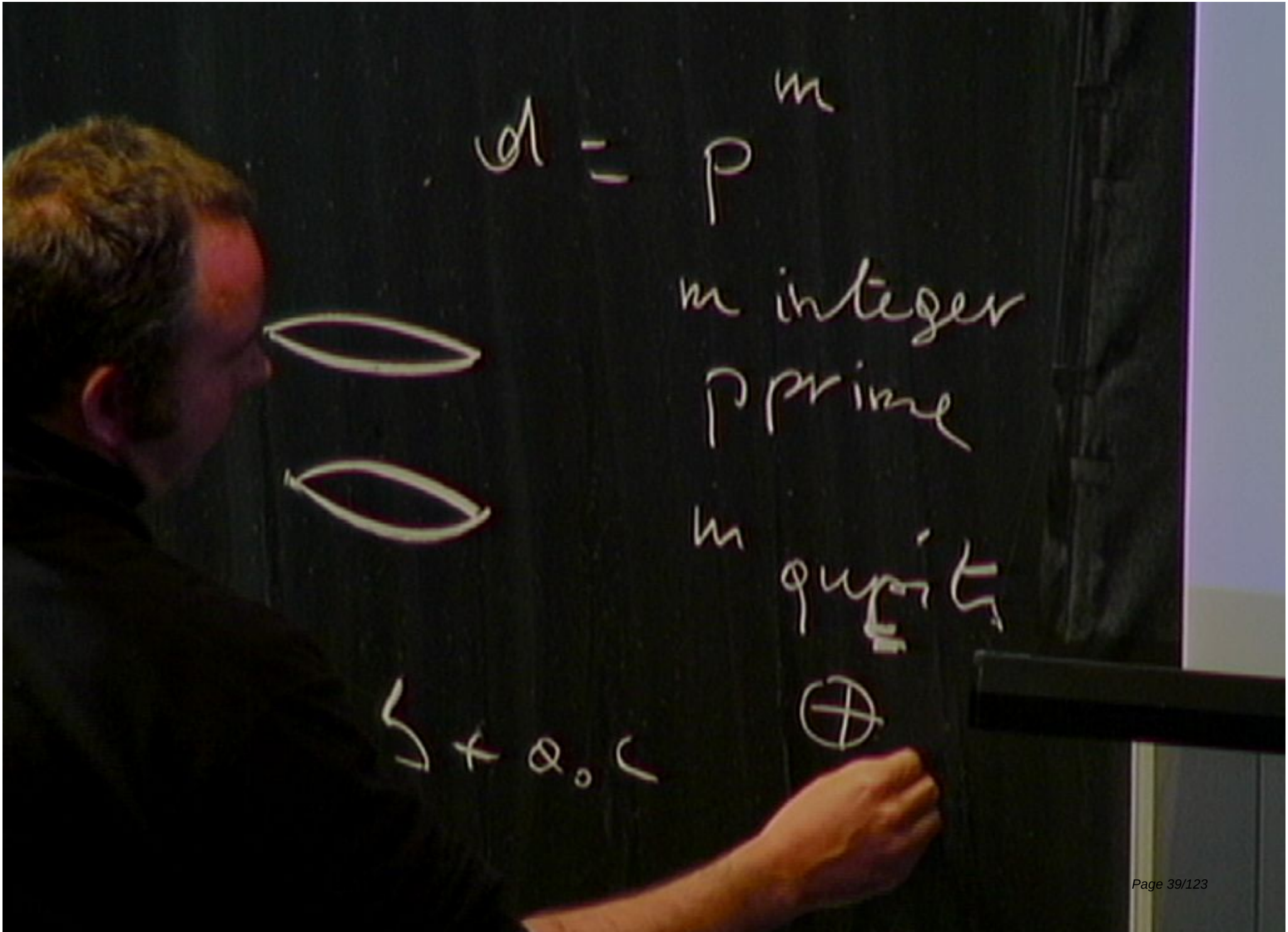
The generalised Pauli group presents numerous applications in Quantum Information (tomograpy, dense coding,teleportation, cloning, error correction and so on). One can show that:

$$\sum_{j=0}^{d-1} \gamma_G^{(j \odot_G i)} = d\delta_{i,0} \tag{6}$$

$$\gamma_G^i \cdot \gamma_G^j = \gamma_G^{(i \oplus_G j)} \tag{7}$$

Besides, the Galois addition factorizes; for instance, in dimension 4, if we express quartits like tensorial products of 2 qubits: $|0\rangle_4 = |0\rangle_2 \otimes |0\rangle_2$, $|1\rangle_4 = |0\rangle_2 \otimes |1\rangle_2$, $|2\rangle_4 = |1\rangle_2 \otimes |0\rangle_2$, $|3\rangle_4 = |1\rangle_2 \otimes |1\rangle_2$,we can check at the level of the addition table that
if $|i\rangle_4 = |i_1\rangle_2 \otimes |i_2\rangle_2$, et $|j\rangle_4 = |j_1\rangle_2 \otimes |j_2\rangle_2$,
then $|i \oplus_G j\rangle_4 = |i_1 \oplus_{mod2} j_1\rangle_2 \otimes |i_2 \oplus_{mod2} j_2\rangle_2$.
This means that the (quartit here) addition FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE. In dimension p^m, with p prime and m a positive integer the Galois addition always FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE.
The Galois multiplication table is more involved but the corresponding tables are well known and are available, for instance on the web.




$q = p^m$
m integer
p prime
m quelconque
$\zeta + \alpha_0 c$

$d = p^m$

m integer

p prime

m qubits

$f(x) = a_0 + a_1 x$ $\oplus \rightarrow$ $+ \bmod p$

The generalised Pauli group presents numerous applications in Quantum Information (tomograpy, dense coding,teleportation, cloning, error correction and so on). One can show that:

$$\sum_{j=0}^{d-1} \gamma_G^{(j \odot_G i)} = d\delta_{i,0} \tag{6}$$

$$\gamma_G^i \cdot \gamma_G^j = \gamma_G^{(i \oplus_G j)} \tag{7}$$

Besides, the Galois addition factorizes; for instance, in dimension 4, if we express quartits like tensorial products of 2 qubits: $|0\rangle_4 = |0\rangle_2 \otimes |0\rangle_2$, $|1\rangle_4 = |0\rangle_2 \otimes |1\rangle_2$, $|2\rangle_4 = |1\rangle_2 \otimes |0\rangle_2$, $|3\rangle_4 = |1\rangle_2 \otimes |1\rangle_2$,we can check at the level of the addition table that
if $|i\rangle_4 = |i_1\rangle_2 \otimes |i_2\rangle_2$, et $|j\rangle_4 = |j_1\rangle_2 \otimes |j_2\rangle_2$,
then $|i \oplus_G j\rangle_4 = |i_1 \oplus_{mod2} j_1\rangle_2 \otimes |i_2 \oplus_{mod2} j_2\rangle_2$.
This means that the (quartit here) addition FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE. In dimension p^m, with p prime and m a positive integer the Galois addition always FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE.
The Galois multiplication table is more involved but the corresponding tables are well known and are available, for instance on the web.

Applications: teleportation and dense coding:

We can now define generalized Bell states as follows:

$$|B_{m^*,n}\rangle = d^{-1/2} \sum_{k=0}^{d-1} \gamma_G^{(k \odot_G n)} |k^*\rangle |k \oplus_G m\rangle \qquad (10)$$

The amplitudes of $|k^*\rangle$ in the reference (computational) basis are defined to be equal to the complex conjugates of the amplitudes of $|k\rangle$.
The equation of **teleportation** is:

$$(\sum_{i=0}^{d-1} \phi_i |i\rangle_A) |B_{0,0}\rangle_{B,C} = \sum_{m,n=0}^{d-1} \frac{1}{d} |B_{m,n}\rangle_{A,B} (V_{m,C}^n (\sum_{i=0}^{d-1} \phi_i |i\rangle_C)) \qquad (11)$$

The equation of **dense coding** is:

$$V_{m,A}^n \otimes 1_B |B_{0,0}\rangle_{A,B} = |B_{m,n}\rangle_{A,B}. \qquad (12)$$

Applications: teleportation and dense coding:

We can now define generalized Bell states as follows:

$$|B_{m^*,n}\rangle = d^{-1/2} \sum_{k=0}^{d-1} \gamma_G^{(k \odot_G n)} |k^*\rangle |k \oplus_G m\rangle \qquad (10)$$

The amplitudes of $|k^*\rangle$ in the reference (computational) basis are defined to be equal to the complex conjugates of the amplitudes of $|k\rangle$.
The equation of **teleportation** is:

$$(\sum_{i=0}^{d-1} \phi_i |i\rangle_A) |B_{0,0}\rangle_{B,C} = \sum_{m,n=0}^{d-1} \frac{1}{d} |B_{m,n}\rangle_{A,B} (V_{m,C}^n (\sum_{i=0}^{d-1} \phi_i |i\rangle_C)) \qquad (11)$$

The equation of **dense coding** is:

$$V_{m,A}^n \otimes 1_B |B_{0,0}\rangle_{A,B} = |B_{m,n}\rangle_{A,B}. \qquad (12)$$

Galois versus modulo.

We can define similarly Bell states through the modulo d ring.
The "teleportation equation" and "dense coding equation" are still valid in those cases.
Nevertheless, if we want to generalize mutually unbiased bases in higher dimensions (MUB's) a field is required.
We can indeed derive $d+1$ MUB's by simultaneously diagonalising well-chosen subgroups of the generalized Pauli group ($V_l^{(i-1)\odot_G l}$).
This technique works only because the Galois operations form a field so that only the Galois operations are convenient therefore.
BESIDES, IT IS WELL-KNOWN THAT FINITE FIELDS ONLY EXIST WHEN THEIR NUMBER OF ELEMENTS IS EQUAL TO A PRIME POWER (p^m with p a prime and m a positive integer) so a set of d +1 MUB's can be built only when d is a prime power.
We found for instance that in ODD prime dimension p^m MUB's can be expressed as follows:

$$|e_k^i\rangle = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \gamma_G^{\ominus_G q \odot_G k} (\gamma_G^{((i-1)\odot_G q \odot_G q)/_G 2}) |e_q^0\rangle \qquad (13)$$

Remarks:
-In even prime power dimensions (2^m m qubits), all is more complicated, because even and odd finite fields are totally different; we find:

$$|e_k^i\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \gamma_G^{\ominus_G q \odot_G k} \Pi_{n=0,q_n\neq 0}^{m-1} i^{(j-1)\odot_G 2^n \odot_G 2^n} \gamma_G^{(j-1)\odot_G 2^n \odot_G 2^{n'}} |e_q^0\rangle, \quad (14)$$

here $q = \sum_{k=0}^{m-1} q_n 2^n$, while n' is the smallest integer strictly superior to n such that $q_{n'} \neq 0$, whenever it exists, 0 otherwise.
-When the dimension of the Hilbert space is not a prime power (for instance $d = 6$) NOBODY KNOWS HOW TO DERIVE $d + 1$ MUB's (open problem). Nobody even knows how many MUB's exist!!!

Application (1): quantum tomography

in prime power dimension $d = p^m$.

As there are $d+1$ MUB's in dimension $d = p^m$, that each von Neumann-measurement of an operator diagonal in a MUB provides $d-1$ independent parameters, and that the results collected in different MUB's are also independent, we get d^2-1 independent parameters.

This is precisely equal to the number of independent parameters that are necessary in order to reconstruct the density matrix of an unknown d-level quantum state. We can thus perform a FULL TOMOGRAPHIC process by measuring transition probabilities in $d+1$ MUB's (W.K. Wootters, and B.D. Fields, "Optimal state-determination by mutually unbiased measurements" Ann. Phys. 191, 363 (1989)).

Example: $d = 2$: we get the $d^2-1 = 3$ Bloch (Stokes) coefficients by measuring the transition probabilities in 3 MUB's (in polarimetry: we measure the populations of circular left and right polarisations, horizontal-vertical and diagonal.)

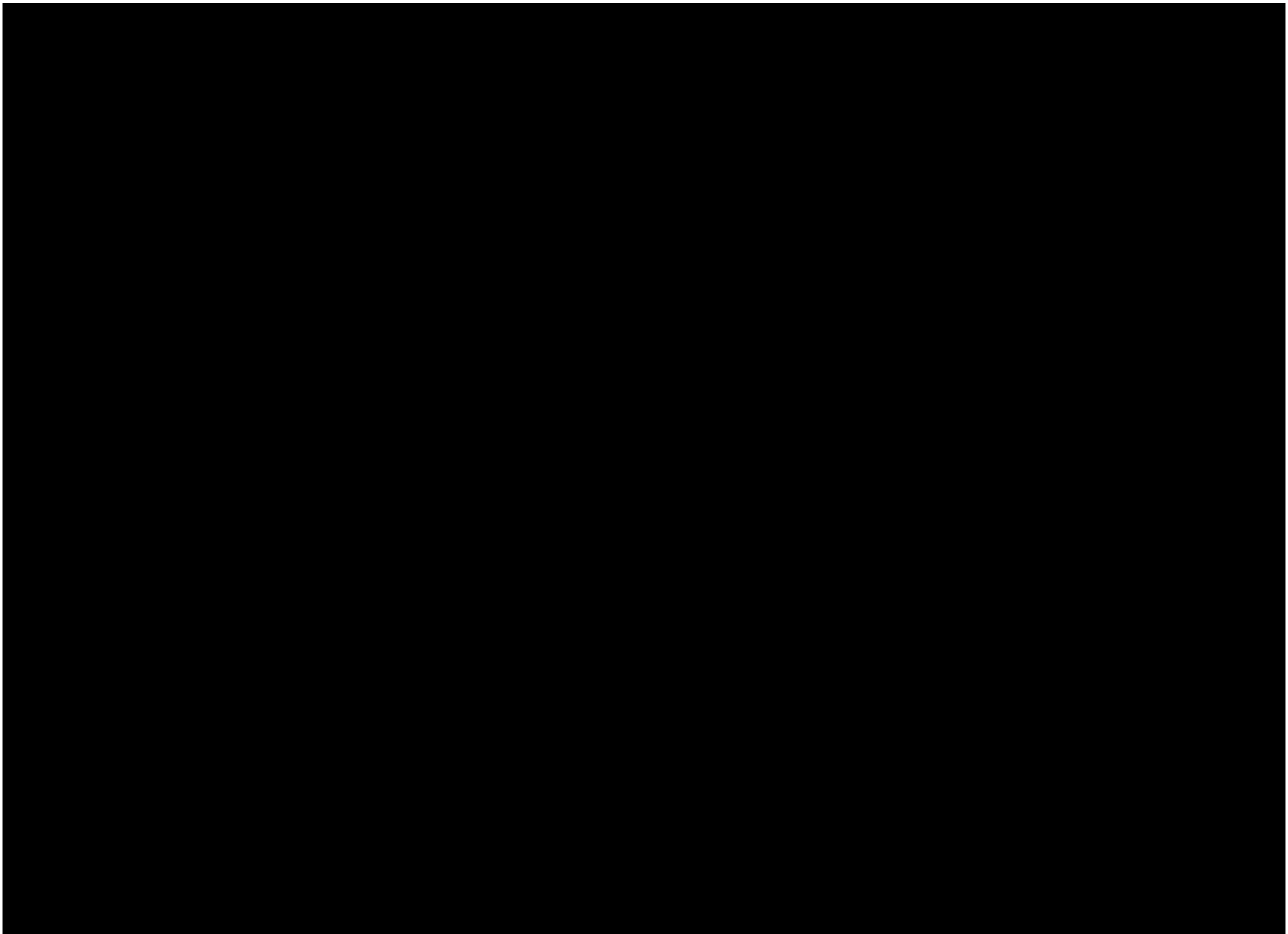
Application (2): Solution of the Mean King's problem

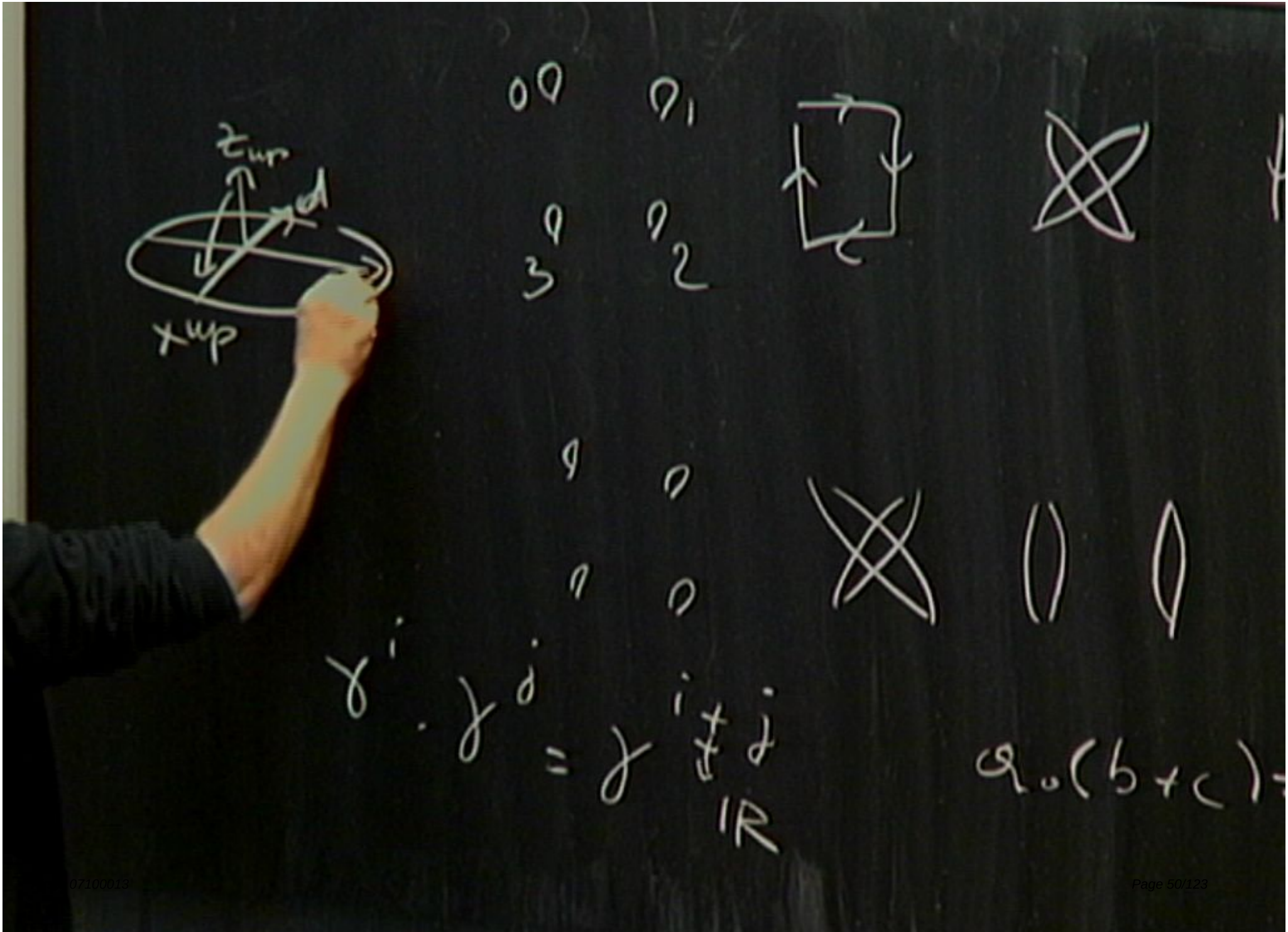
in prime power dimension $d = p^m$.

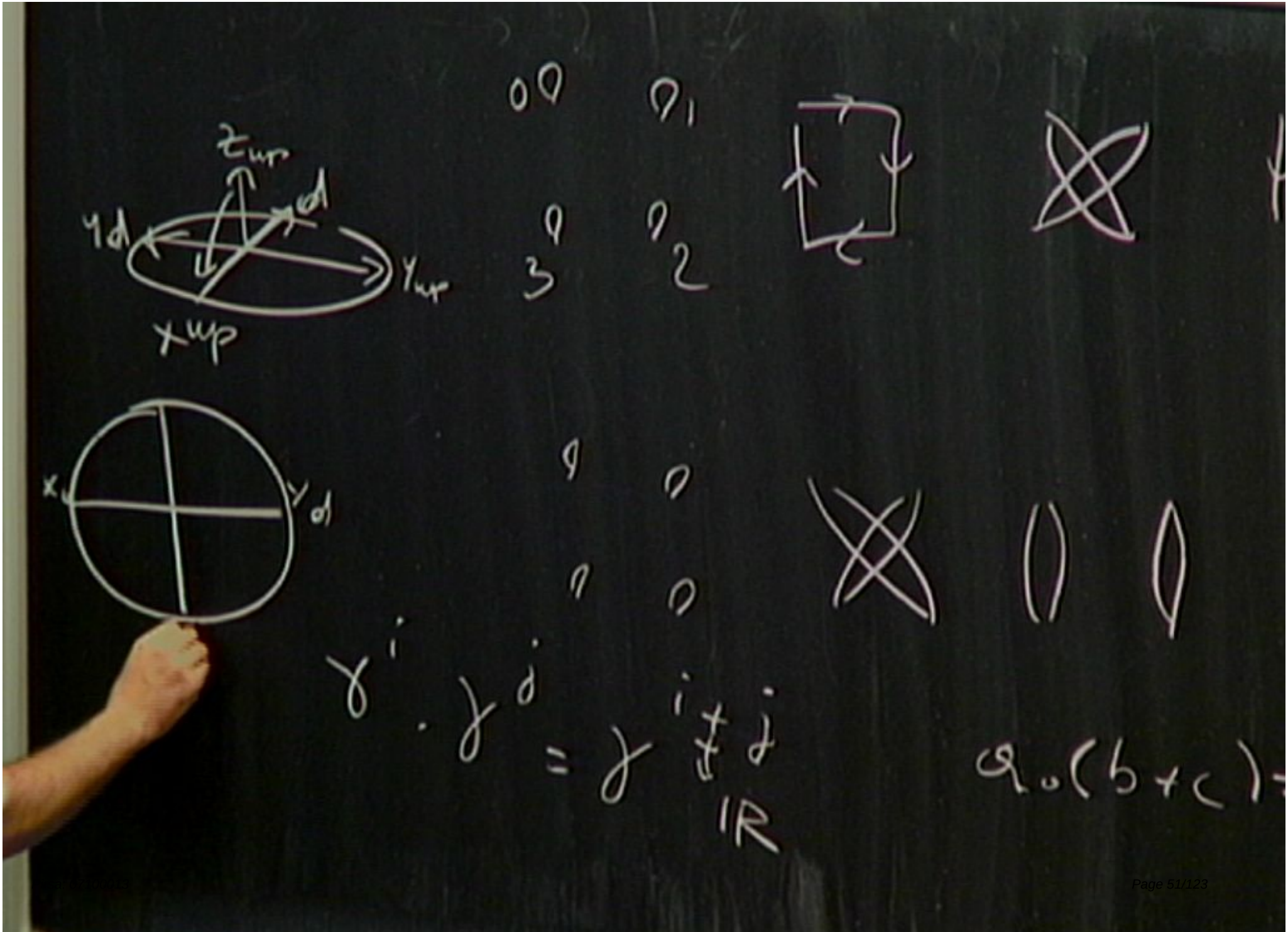
A. $d = 2$ Vaidman-Aharonov 1987:
Is it possible to ascertain the spin component of a spin 1/2 particle along 3 complementary directions?

A Mean King challenges a physicist, Alice, who got stranded on the remote island ruled by the king, to prepare a spin1/2 atom in any state of her choosing and to perform a control measurement of her liking. Between her preparation and her measurement, the king's men determine the value of either σ_X, σ_Y or σ_Z. Only after she completed the control measurement, the physicist is told which spin component has been measured, and she must then state the result of that intermediate measurement correctly. How does she do it?

A priori, no solution: if Alice has only one qubit at her disposal, the optimal strategy consists of preparing a pure state polarised along one of the 3 directions (for instance Z); thereafter, when the Mean King performs his measure Alice can still measure the spin along a direction in-between X and Y (Breidbart basis), which allows her to infer correctly the spin value along X or Y with a probability equal to $cos^2(22.5) \approx 0,85$. In average Alice infers correctly the spin value with a probability $\approx 0,9 = (1 + 2.0.85)/3$.
Nevertheless, a solution of the problem exists, provided we make use of the resources provided by entanglement (Vaidman et al. 1987). One can express this solution elegantly in function of Bell states as we shall now show .




z_{up}
x_{up}
$\gamma^i \cdot \gamma^j = \gamma^{i \neq j}$
IR


z_{up}
y_{down}
y_{up}
x_{up}
x_{down}
y_{down}
$\gamma^i \cdot \gamma^j = \gamma^{i \neq j}$
IR
$q \cdot (b + c)$

A priori, no solution: if Alice has only one qubit at her disposal, the optimal strategy consists of preparing a pure state polarised along one of the 3 directions (for instance Z); thereafter, when the Mean King performs his measure Alice can still measure the spin along a direction in-between X and Y (Breidbart basis), which allows her to infer correctly the spin value along X or Y with a probability equal to $cos^2(22.5) \approx 0,85$. In average Alice infers correctly the spin value with a probability $\approx 0,9 = (1 + 2.0.85)/3$.
Nevertheless, a solution of the problem exists, provided we make use of the resources provided by entanglement (Vaidman et al. 1987). One can express this solution elegantly in function of Bell states as we shall now show .

Alice's strategy is the following.
She prepares two entangled qubits (one for her one for the King) in the Bell state: $B^Z{}_{00} = \frac{1}{\sqrt{2}}(|0\rangle^Z_A|0\rangle^Z_K + |1\rangle^Z_A|1\rangle^Z_K)$
This state, as well as other Bell states, is "covariant" when it is reexpressed in the two other MUB's (along X and Y):

$$
\begin{aligned}
|B^Z_{0,0}\rangle_{A,K} &= |B^X_{0,0}\rangle_{A,K} = |B^Y_{0^*,0}\rangle_{A,K} \\
|B^Z_{0,1}\rangle_{A,K} &= |B^X_{1,0}\rangle_{A,K} = |B^Y_{1^*,0}\rangle_{A,K} \\
|B^Z_{1,0}\rangle_{A,K} &= |B^X_{0,1}\rangle_{A,K} = i|B^Y_{1^*,1}\rangle_{A,K} \\
|B^Z_{1,1}\rangle_{A,K} &= -|B^X_{1,1}\rangle_{A,K} = (-i)|B^Y_{0^*,1}\rangle_{A,K}
\end{aligned}
\qquad (15)
$$

During his measurement the King projects thus the initial state prepared by Alice onto one of the 6 product states:
$|0\rangle^X_{King} \otimes |0\rangle^X_{Alice}$,, or $|1\rangle^X_{King} \otimes |1\rangle^X_{Alice}$,
$|0\rangle^y_{King} \otimes |0*\rangle^y_{Alice}$, or $|1\rangle^Y_{King} \otimes |1*\rangle^Y_{Alice}$,
$|0\rangle^Z_{King} \otimes |0\rangle^Z_{Alice}$, or $|1\rangle^Z_{King} \otimes |1\rangle^Z_{Alice}$,
the job of Alice consists of DISCRIMINATING those 6 product-states.

She can discriminate between those 6 states with CERTAINTY 1 by measuring them in the following basis:

$$|\Psi\rangle_1^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K}) \quad (16)$$

$$|\Psi\rangle_2^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_3^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_4^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K})$$

Indeed, as $|B\rangle_{00} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ and $|B\rangle_{01} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$, whenever one of the two first (last) detectors clicks, and that the King measured in the Z basis, he certainly observed the result 0 (1), because the corresponding projectors are orthogonal to $|1\rangle_K^Z|1\rangle_A^Z$ ($|0\rangle_K^Z|0\rangle_A^Z$).

By covariance this result generalizes to the 2 other directions (X and Y).

Alice's strategy is the following.
She prepares two entangled qubits (one for her one for the King) in the Bell state: $B^Z{}_{00} = \frac{1}{\sqrt{2}}(|0\rangle^Z_A|0\rangle^Z_K + |1\rangle^Z_A|1\rangle^Z_K)$
This state, as well as other Bell states, is "covariant" when it is reexpressed in the two other MUB's (along X and Y):

$$
\begin{aligned}
|B^Z_{0,0}\rangle_{A,K} &= |B^X_{0,0}\rangle_{A,K} = |B^Y_{0^*,0}\rangle_{A,K} \\
|B^Z_{0,1}\rangle_{A,K} &= |B^X_{1,0}\rangle_{A,K} = |B^Y_{1^*,0}\rangle_{A,K} \\
|B^Z_{1,0}\rangle_{A,K} &= |B^X_{0,1}\rangle_{A,K} = i|B^Y_{1^*,1}\rangle_{A,K} \\
|B^Z_{1,1}\rangle_{A,K} &= -|B^X_{1,1}\rangle_{A,K} = (-i)|B^Y_{0^*,1}\rangle_{A,K} \qquad (15)
\end{aligned}
$$

During his measurement the King projects thus the initial state prepared by Alice onto one of the 6 product states:
$|0\rangle^X_{King} \otimes |0\rangle^X_{Alice}$,, or $|1\rangle^X_{King} \otimes |1\rangle^X_{Alice}$,
$|0\rangle^y_{King} \otimes |0*\rangle^y_{Alice}$, or $|1\rangle^Y_{King} \otimes |1*\rangle^Y_{Alice}$,
$|0\rangle^Z_{King} \otimes |0\rangle^Z_{Alice}$, or $|1\rangle^Z_{King} \otimes |1\rangle^Z_{Alice}$,
the job of Alice consists of DISCRIMINATING those 6 product-states.

She can discriminate between those 6 states with CERTAINTY 1 by measuring them in the following basis:

$$|\Psi\rangle_1^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K}) \quad (16)$$

$$|\Psi\rangle_2^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_3^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_4^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K})$$

Indeed, as $|B\rangle_{00} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ and $|B\rangle_{01} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$, whenever one of the two first (last) detectors clicks, and that the King measured in the Z basis, he certainly observed the result 0 (1), because the corresponding projectors are orthogonal to $|1\rangle_K^Z|1\rangle_A^Z$ ($|0\rangle_K^Z|0\rangle_A^Z$).

By covariance this result generalizes to the 2 other directions (X and Y).

Alice's strategy is the following.
She prepares two entangled qubits (one for her one for the King) in the Bell state: $B^Z{}_{00} = \frac{1}{\sqrt{2}}(|0\rangle^Z_A|0\rangle^Z_K + |1\rangle^Z_A|1\rangle^Z_K)$
This state, as well as other Bell states, is "covariant" when it is reexpressed in the two other MUB's (along X and Y):

$$\begin{aligned}
|B^Z_{0,0}\rangle_{A,K} &= |B^X_{0,0}\rangle_{A,K} = |B^Y_{0^*,0}\rangle_{A,K} \\
|B^Z_{0,1}\rangle_{A,K} &= |B^X_{1,0}\rangle_{A,K} = |B^Y_{1^*,0}\rangle_{A,K} \\
|B^Z_{1,0}\rangle_{A,K} &= |B^X_{0,1}\rangle_{A,K} = i|B^Y_{1^*,1}\rangle_{A,K} \\
|B^Z_{1,1}\rangle_{A,K} &= -|B^X_{1,1}\rangle_{A,K} = (-i)|B^Y_{0^*,1}\rangle_{A,K} \qquad (15)
\end{aligned}$$

During his measurement the King projects thus the initial state prepared by Alice onto one of the 6 product states:
$|0\rangle^X_{King} \otimes |0\rangle^X_{Alice}$,, or $|1\rangle^X_{King} \otimes |1\rangle^X_{Alice}$,
$|0\rangle^y_{King} \otimes |0*\rangle^y_{Alice}$, or $|1\rangle^Y_{King} \otimes |1*\rangle^Y_{Alice}$,
$|0\rangle^Z_{King} \otimes |0\rangle^Z_{Alice}$, or $|1\rangle^Z_{King} \otimes |1\rangle^Z_{Alice}$,
the job of Alice consists of DISCRIMINATING those 6 product-states.

She can discriminate between those 6 states with CERTAINTY 1 by measuring them in the following basis:

$$|\Psi\rangle_1^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K}) \quad (16)$$

$$|\Psi\rangle_2^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_3^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_4^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K})$$

Indeed, as $|B\rangle_{00} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ and $|B\rangle_{01} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$, whenever one of the two first (last) detectors clicks, and that the King measured in the Z basis, he certainly observed the result 0 (1), because the corresponding projectors are orthogonal to $|1\rangle_K^Z|1\rangle_A^Z$ ($|0\rangle_K^Z|0\rangle_A^Z$).

By covariance this result generalizes to the 2 other directions (X and Y).

B. Generalisation in dimension p^m (T. Durt: "About the Mean King's problem and discrete Wigner distributions", International Journal of Modern Physics B, 20, 11-13, 1742-1760 (2006)).

The covariance of Bell states reflects the properties of Clifford group; it can be generalized to higher prime power dimensions p^m:

$$|B^0_{m^*,n}\rangle = \gamma_G^{(\ominus_G m \odot_G n)} \cdot (\gamma_G^{((k-1)\odot_G m \odot_G m)})^{\frac{1}{2}} |B^k_{(\ominus_G n \oplus_G (k-1)\odot_G m)^*,m}\rangle,$$

$(k-1) = 0 - d - 1$

The two-qubit basis used by Alice also generalizes:

$$|\Psi\rangle^0_{(i_1,i_2)} = \frac{1}{d}\left(\sum_{m,n=0}^{d-1} \gamma_G^{(i_1,i_2)\odot\odot_G(m,n)} (\gamma_G^{(m\odot_G n)})^{\frac{1}{2}} |B^0_{m,n}\rangle_{K,A}\right)$$

here $\odot\odot_G$ represents the quadratic extension of Galois multiplication, that can be obtained on the basis of the field with d elements by adding a new element (in the same way that complex numbers can be derived from real numbers by adding a new element i, the square root of -1.

Application (3): Wigner distribution

in prime power dimensions p^m.

We have seen before that displacement operators are in 1-1 correspondence with Bell states.

Similarly, the measurement basis associated to the resolution of the Mean King's problem is in 1-1 correspondence with a basis of linear qu*d*it operators.

It appears that these operators form a DISCRETE COUNTERPART of continuous WIGNER OPERATORS-they are thus DISCRETE PHASE-SPACE LOCALISATION OPERATORS (T. Durt: "About the Mean King's problem and discrete Wigner distributions", International Journal of Modern Physics B, 20, 11-13, 1742-1760 (2006)).

B. Generalisation in dimension p^m (T. Durt: "About the Mean King's problem and discrete Wigner distributions", International Journal of Modern Physics B, 20, 11-13, 1742-1760 (2006)).

The covariance of Bell states reflects the properties of Clifford group; it can be generalized to higher prime power dimensions p^m:

$$|B^0_{m^*,n}\rangle = \gamma_G^{(\ominus_G m \odot_G n)} \cdot (\gamma_G^{((k-1)\odot_G m \odot_G m)})^{\frac{1}{2}} |B^k_{(\ominus_G n \oplus_G (k-1)\odot_G m)^*,m}\rangle,$$

$(k-1) = 0 - d - 1$

The two-qubit basis used by Alice also generalizes:

$$|\Psi\rangle^0_{(i_1,i_2)} = \frac{1}{d}\left(\sum_{m,n=0}^{d-1} \gamma_G^{(i_1,i_2)\odot\odot_G(m,n)} (\gamma_G^{(m\odot_G n)})^{\frac{1}{2}} |B^0_{m,n}\rangle_{K,A}\right)$$

here $\odot\odot_G$ represents the quadratic extension of Galois multiplication, that can be obtained on the basis of the field with d elements by adding a new element (in the same way that complex numbers can be derived from real numbers by adding a new element i, the square root of -1.

Application (3): Wigner distribution

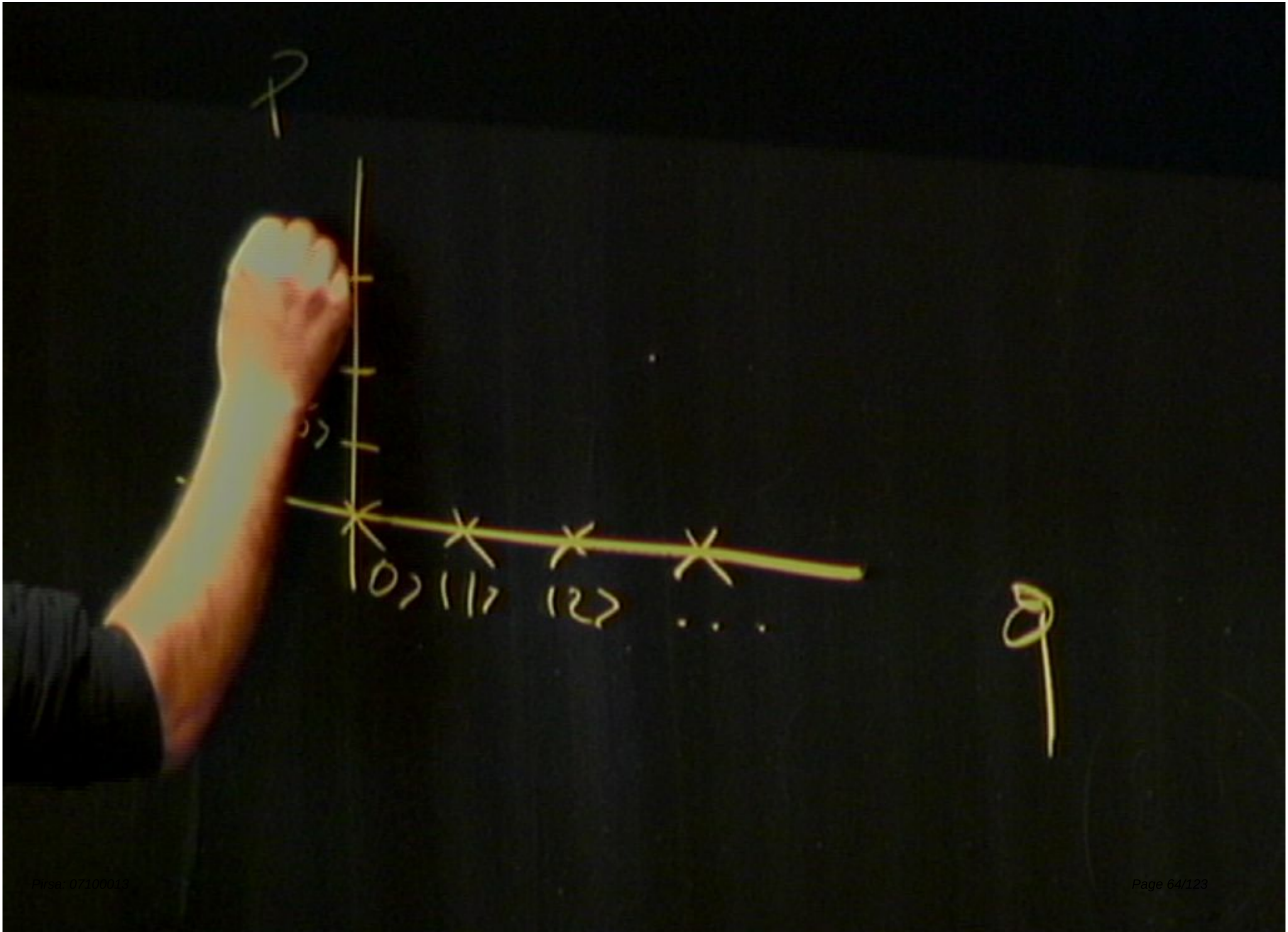
in prime power dimensions p^m.

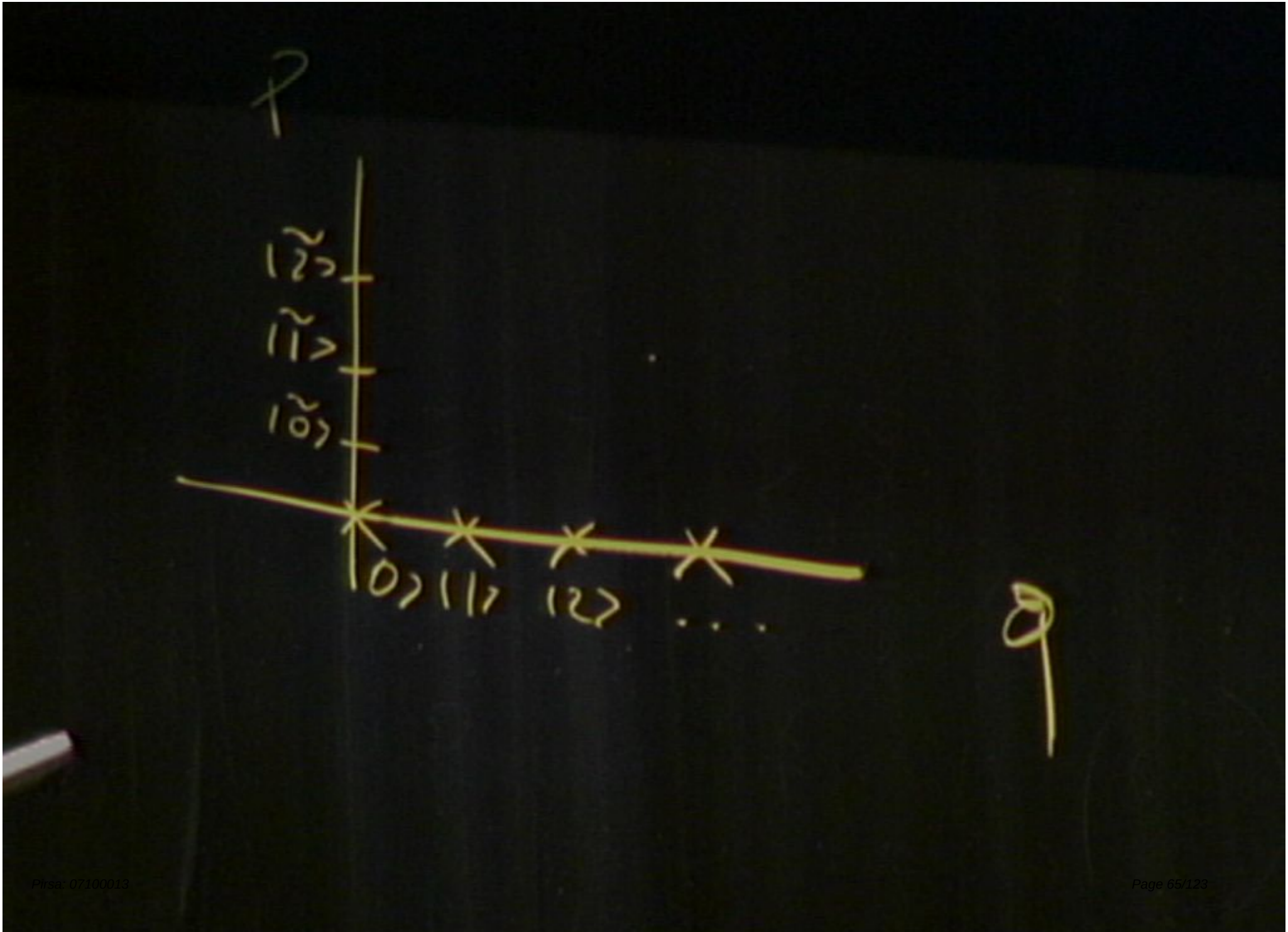
We have seen before that displacement operators are in 1-1 correspondence with Bell states.

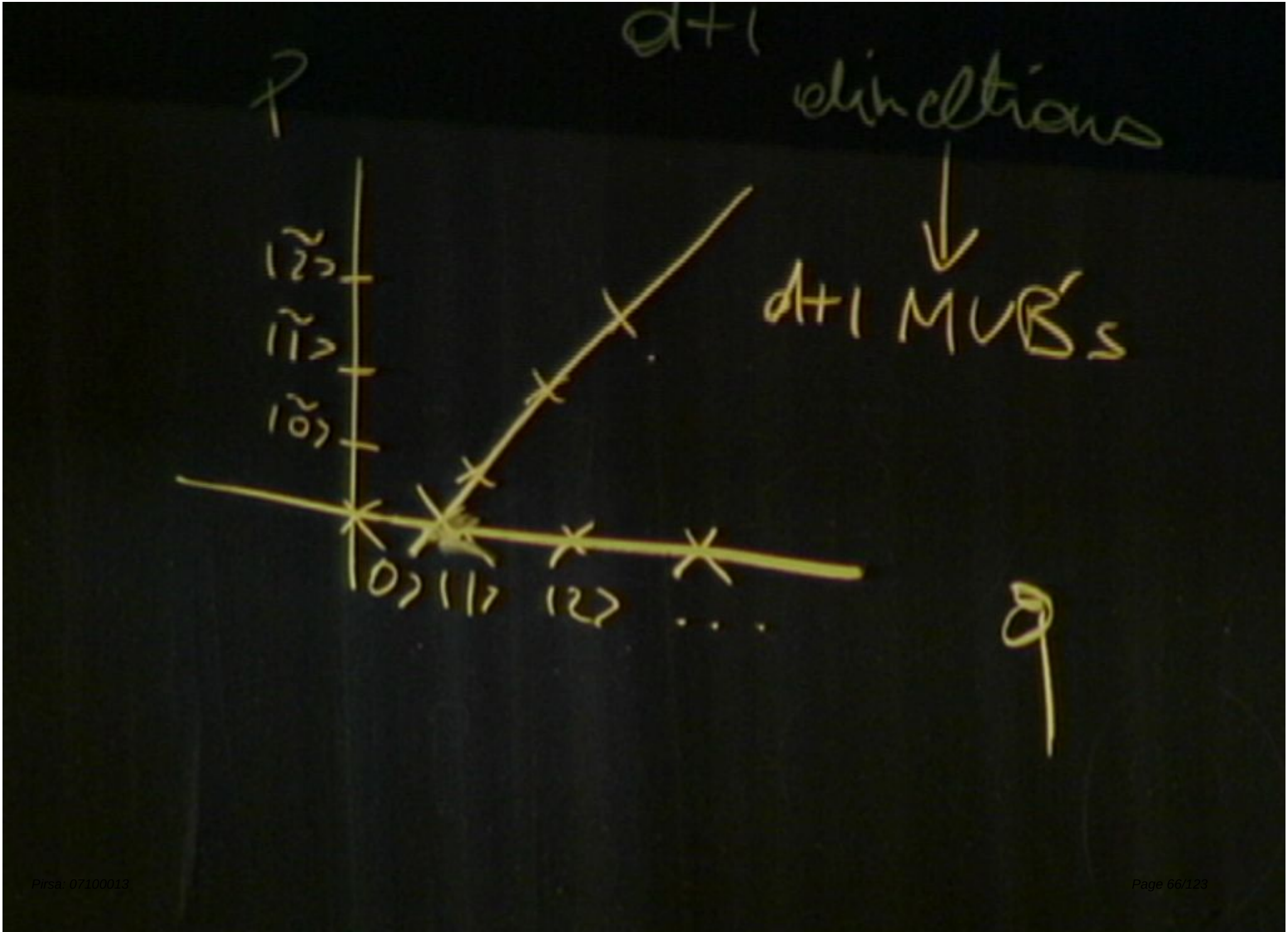
Similarly, the measurement basis associated to the resolution of the Mean King's problem is in 1-1 correspondence with a basis of linear qu*d*it operators.

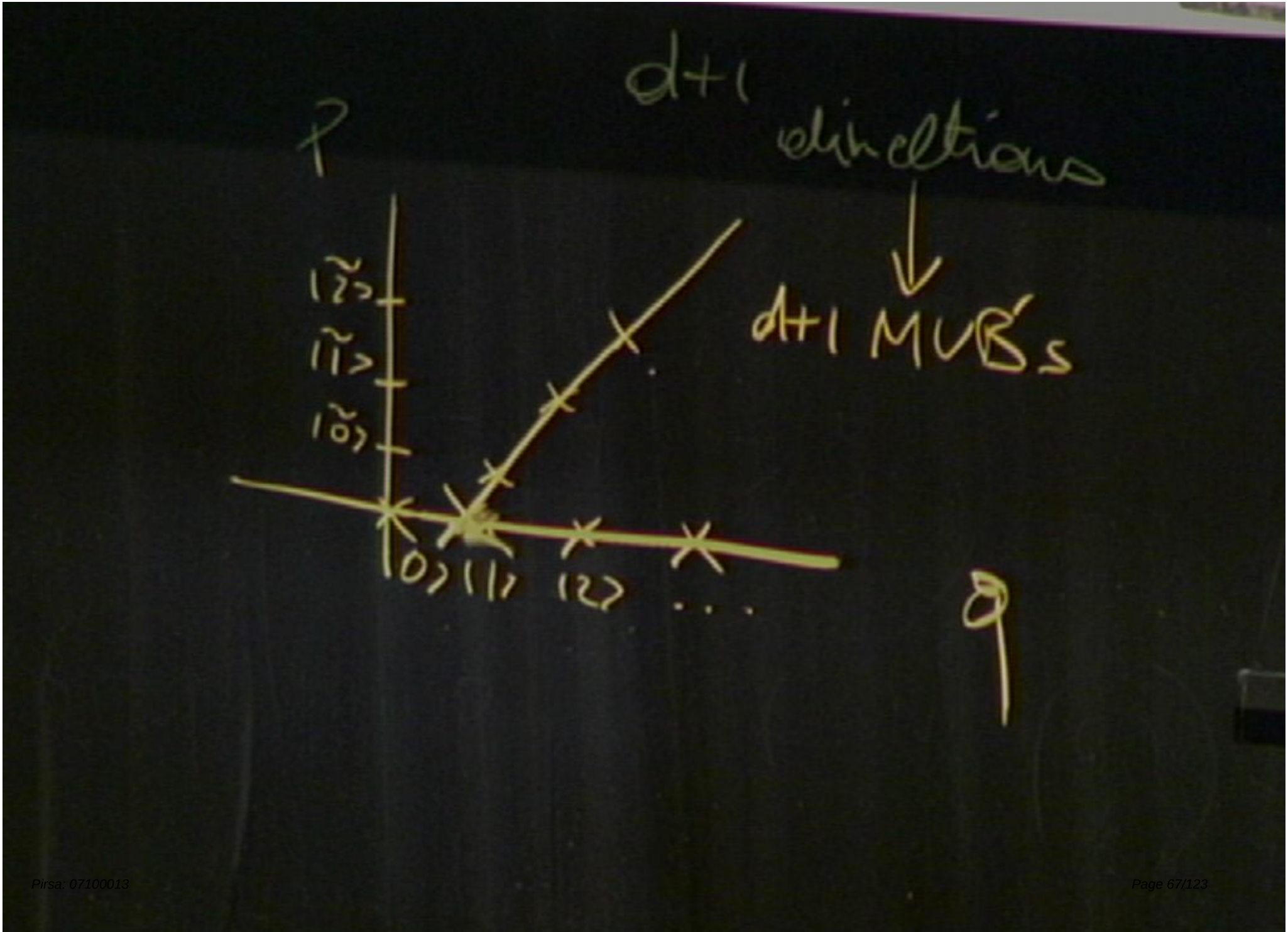
It appears that these operators form a DISCRETE COUNTERPART of continuous WIGNER OPERATORS-they are thus DISCRETE PHASE-SPACE LOCALISATION OPERATORS (T. Durt: "About the Mean King's problem and discrete Wigner distributions", International Journal of Modern Physics B, 20, 11-13, 1742-1760 (2006)).

Wigner distribution is equal to the average value of Wigner operators.
As its continuous counterparts it obeys the following constraints (W.K. Wootters, "Picturing qubits in phase-space", IBM Journal of Research and Development archive Volume 48, Issue 1 (January 2004), quant-ph/0406032 (2004)):
(a) Translational invariance: $W_{(i_1,i_2)} = (V_{i_1}^{i_2})^{\dagger} W_{(0,0)} V_{i_1}^{i_2}$;
(b) The sum of the d^2 Wigner amplitudes $Tr.\rho.W_{(i_1,i_2)}$ is normalized to unity;
(c) Marginals: if we consider STRAIGHT LINES in phase-space defined by the relations $a \odot_G i_1 = b \odot_G i_2 \oplus_G c$, with a b and c elements of the finite (Galois) field with d elements, the averages of Wigner operators along such lines (marginals) are equal to a projector onto one of the MUB's states.
Moreover, marginals along non-intersecting parallel lines correspond to projectors onto orthogonal states of a same MUB while marginals taken along non-parallel directions correspond to projectors onto states from different MUB's.

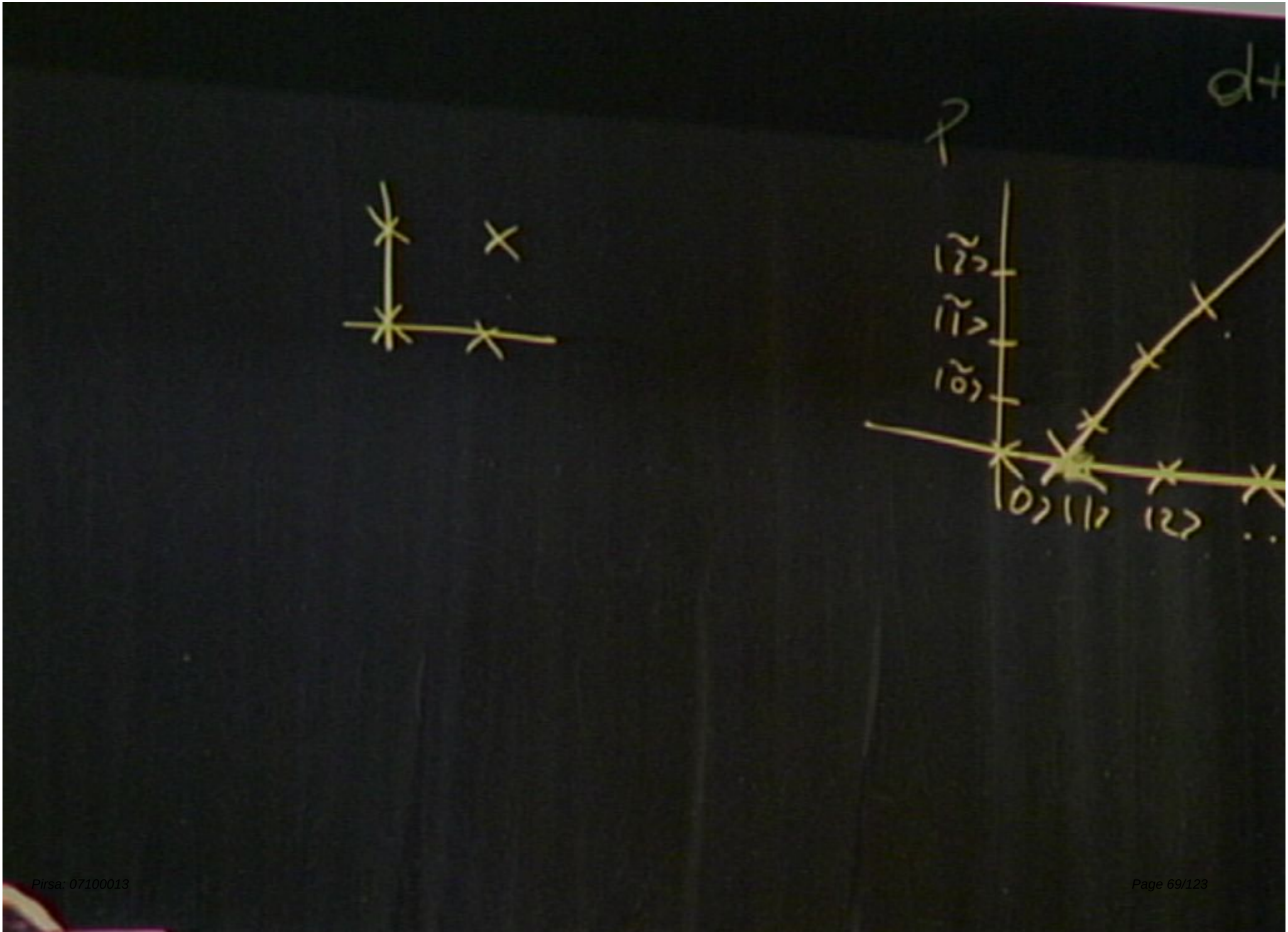

P
|0⟩ |1⟩ |2⟩ . . .
g

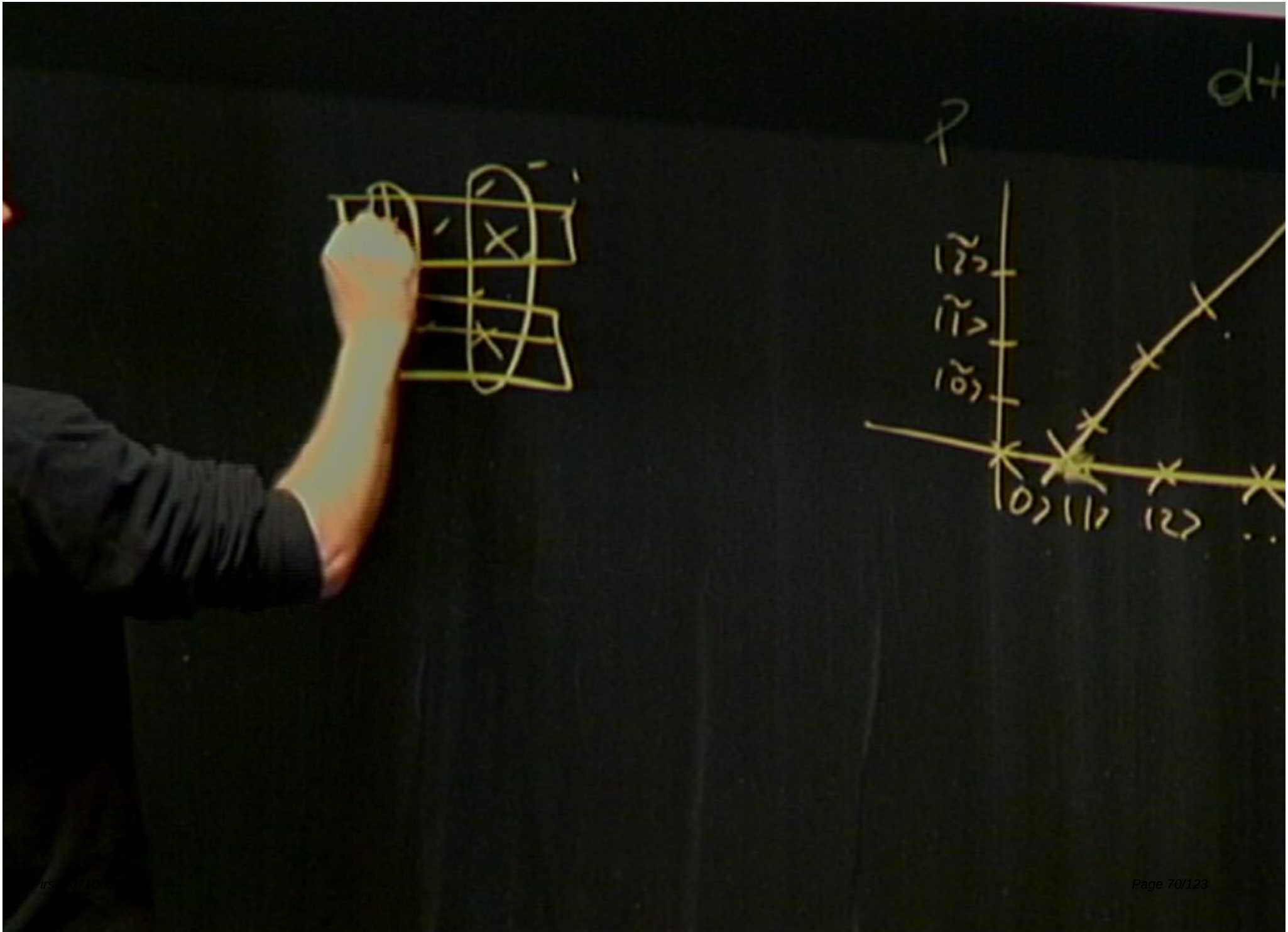

p
|2̃⟩
|1̃⟩
|0̃⟩
|0⟩ |1⟩ |2⟩ . . .
q

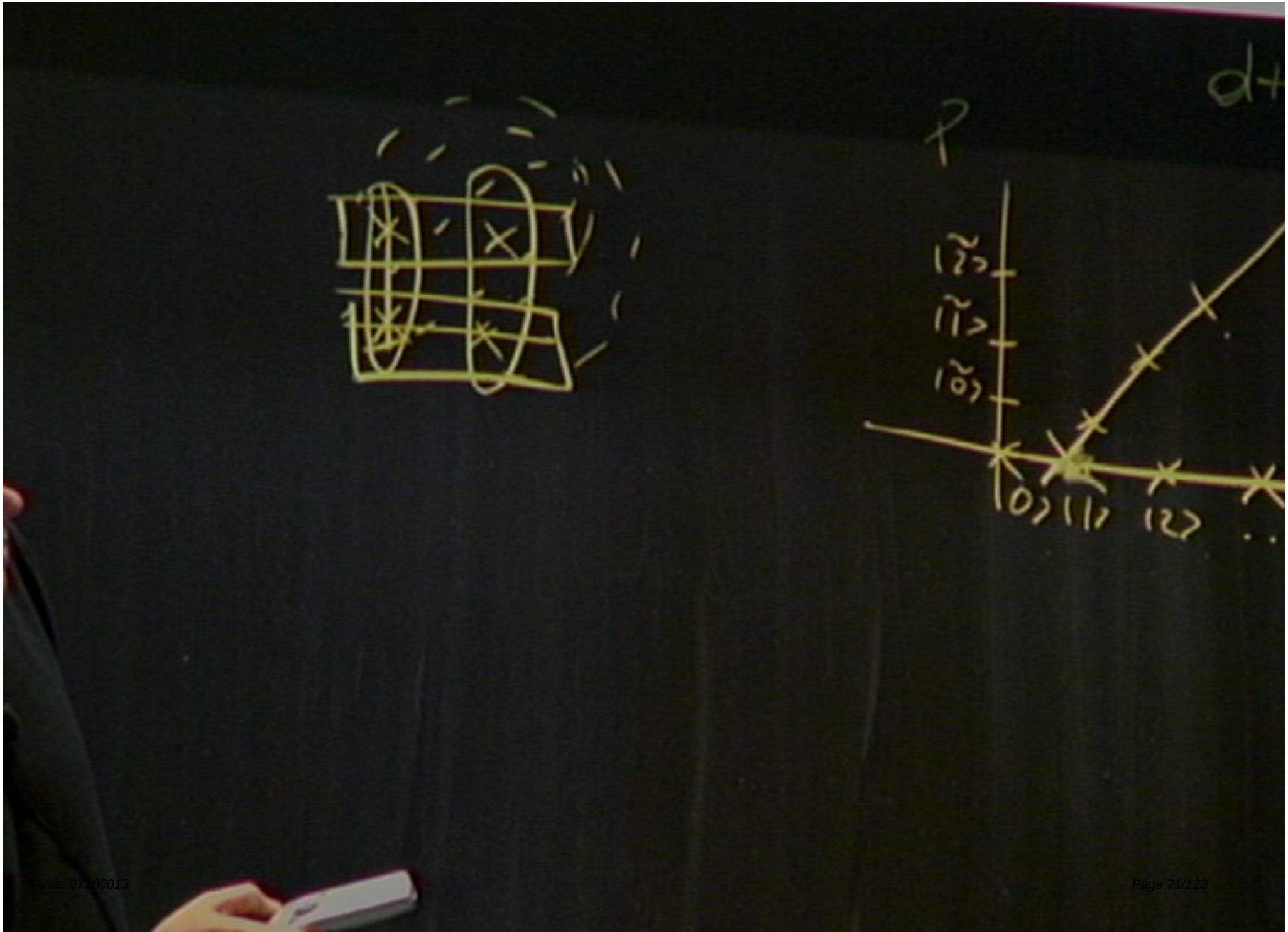

d+1
P
directions
d+1 MUBs
|2̃⟩
|1̃⟩
|0̃⟩
|0⟩ |1⟩ |2⟩ . . .
q


d+1
directions
P
d+1 MUBs
|2̃⟩
|1̃⟩
|0̃⟩
|0⟩ |1⟩ |2⟩ ...
q

Example: the simplest case $d = 2$:
$W_{0,0} + W_{0,1} + W_{1,0} + W_{1,1} = Id.$ by normalisation;
in virtue of the marginal's properties:
$W_{0,0}+W_{0,1}$ and $W_{1,0}+W_{11}$ are projectors onto eigenstates of σ_X, while $W_{0,0}+W_{1,0}$ and $W_{0,1} + W_{1,1}$ are projectors onto eigenstates of σ_Z
Finally $W_{0,0} + W_{1,1}$ and $W_{1,0} + W_{0,1}$ are projectors onto eigenstates of σ_Y.
We can choose such states to be up (0) or down (1), so that: $(W_{0,0} + W_{0,1}) + (W_{0,0} + W_{1,0}) + (W_{0,0} + W_{1,1}) = \frac{1}{2}(Id.(+/-)_X\sigma_X) + \frac{1}{2}(Id.(+/-)_Y\sigma_Y) + \frac{1}{2}(Id.(+/-)_Z\sigma_Z) = 4.W_{0,0} + Id.$


d+
P
|2̃⟩
|1̃⟩
|0̃⟩
|0⟩ |1⟩ |2⟩


P
|2̃⟩
|1̃⟩
|0̃⟩
|0⟩ |1⟩ |2⟩


P
|2>
|1>
|0>
|0> |1> |2>

Example: the simplest case $d = 2$:
$W_{0,0} + W_{0,1} + W_{1,0} + W_{1,1} = Id.$ by normalisation;
in virtue of the marginal's properties:
$W_{0,0}+W_{0,1}$ and $W_{1,0}+W_{11}$ are projectors onto eigenstates of σ_X, while $W_{0,0}+W_{1,0}$ and $W_{0,1} + W_{1,1}$ are projectors onto eigenstates of σ_Z
Finally $W_{0,0} + W_{1,1}$ and $W_{1,0} + W_{0,1}$ are projectors onto eigenstates of σ_Y.
We can choose such states to be up (0) or down (1), so that: $(W_{0,0} + W_{0,1}) + (W_{0,0} + W_{1,0}) + (W_{0,0} + W_{1,1}) = \frac{1}{2}(Id.(+/-)_X\sigma_X) + \frac{1}{2}(Id.(+/-)_Y\sigma_Y) + \frac{1}{2}(Id.(+/-)_Z\sigma_Z) = 4.W_{0,0} + Id.$

Once we fix the phases $+/-$ we can derive Wigner operators. Let us for instance choose the + value everywhere, we obtain so the following candidate for the Wigner distribution (expressed in function of Bloch-Stokes parameters)

$$\begin{cases} P_{00} = \frac{1}{4}[1 + p_X + p_Y + p_Z] = \frac{1}{4} < \sigma_0 + \sigma_x + \sigma_y + \sigma_z > \\ P_{01} = \frac{1}{4}[1 - p_X - p_Y + p_Z] = \frac{1}{4} < \sigma_0 - \sigma_x - \sigma_y + \sigma_z > \\ P_{10} = \frac{1}{4}[1 + p_X - p_Y - p_Z] = \frac{1}{4} < \sigma_0 + \sigma_x - \sigma_y - \sigma_z > \\ P_{11} = \frac{1}{4}[1 - p_X + p_Y - p_Z] = \frac{1}{4} < \sigma_0 - \sigma_x + \sigma_y - \sigma_z > \end{cases} \quad (17)$$

-THIS IS DIRECTLY RELATED TO THE SOLUTION OF THE QUBIT MEAN KING's PROBLEM (EQN.16) :

$$|\Psi\rangle_1^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_2^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_3^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_4^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K})$$

Once we fix the phases $+/-$ we can derive Wigner operators. Let us for instance choose the + value everywhere, we obtain so the following candidate for the Wigner distribution (expressed in function of Bloch-Stokes parameters)

$$\begin{cases} P_{00} = \frac{1}{4}[1 + p_X + p_Y + p_Z] = \frac{1}{4} < \sigma_0 + \sigma_x + \sigma_y + \sigma_z > \\ P_{01} = \frac{1}{4}[1 - p_X - p_Y + p_Z] = \frac{1}{4} < \sigma_0 - \sigma_x - \sigma_y + \sigma_z > \\ P_{10} = \frac{1}{4}[1 + p_X - p_Y - p_Z] = \frac{1}{4} < \sigma_0 + \sigma_x - \sigma_y - \sigma_z > \\ P_{11} = \frac{1}{4}[1 - p_X + p_Y - p_Z] = \frac{1}{4} < \sigma_0 - \sigma_x + \sigma_y - \sigma_z > \end{cases} \quad (17)$$

-THIS IS DIRECTLY RELATED TO THE SOLUTION OF THE QUBIT MEAN KING's PROBLEM (EQN.16) :

$$|\Psi\rangle_1^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_2^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_3^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})$$

$$|\Psi\rangle_4^Z = \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K})$$

Recently, the qubit Wigner distribution has been measured through a SIC POVM measurement on a 2 qubit RMN system by chinese experimentalist colleagues (J-F Du, T. Durt et al., in collaboration with NUS Singapore, and Hefei Quantum Information group, China, Physical Review A 2006).
The 2 qubit Wigner distribution has also been measured on entangled in polarisation photon pairs through two simultaneous local SIC POVM measurements at NUS (Durt, Ling, Lammas-Linares and Kurtsiefer-submitted to PRA).

Appendix: Epistemic interpretation

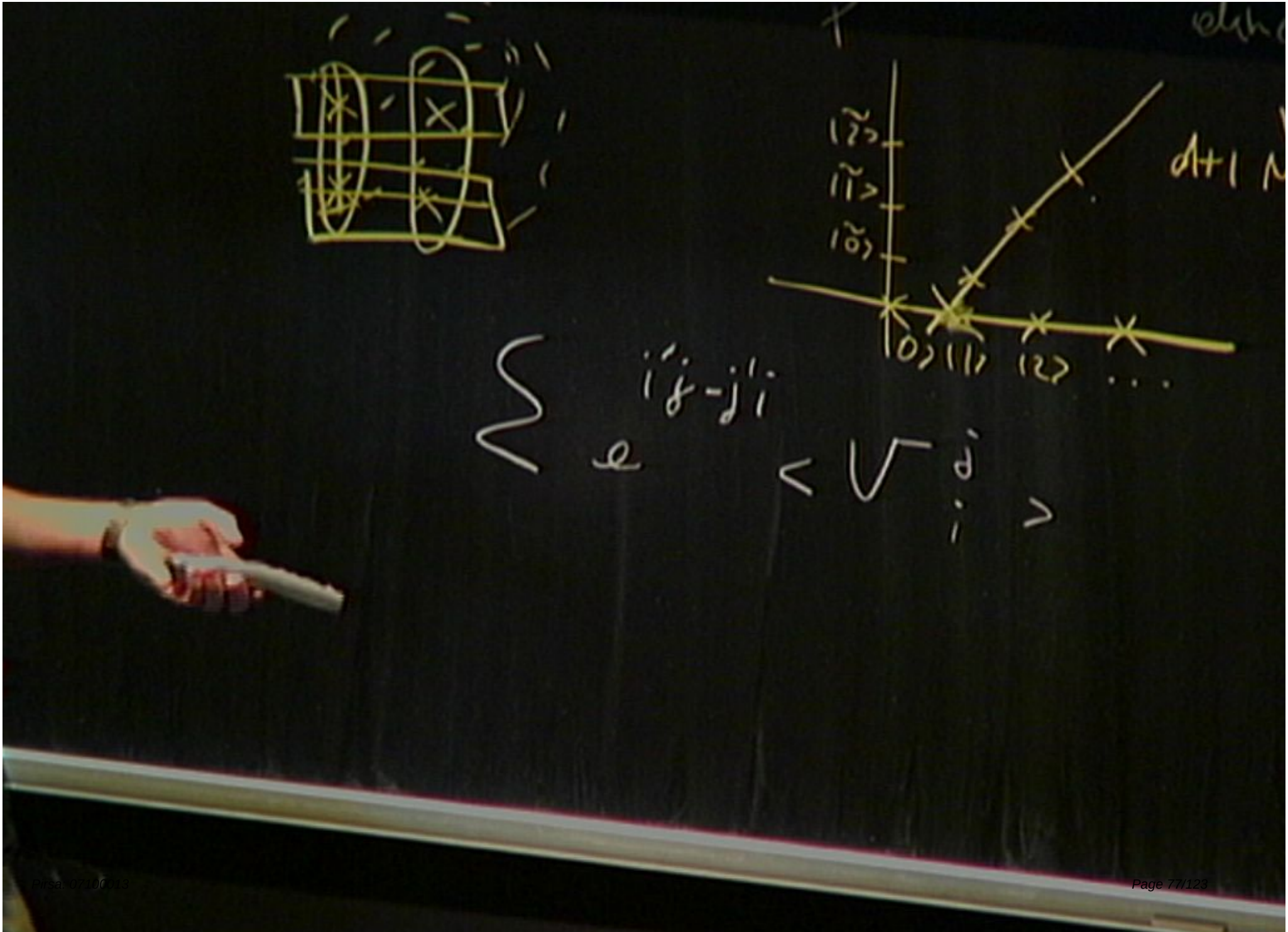
and the role of dimensions.

-The labels of the Wigner operators form a d times d square that plays the role of a discrete phase space.

-The horizontal and the vertical axes correspond to a discrete version of the position-impulsion representations.

-Then, in virtue of the marginal property, we have that each vertical line of the square (there are d of them) corresponds to a state of the computational basis, each horizontal line corresponds to a state of the dual (Galois-Fourier) basis and more generally each set of parallel straight lines corresponds to a state of one of the MUB's.

-This property agrees with the fact that when the Mean King prepares such a state d detectors among d^2 detectors are likely to fire, with the same probability, which reflects a complementary relation between pairs of MUB's.


|2>
|1>
|0>
d+1
|0> |1> |2> ...
Σ e^{i'j-j'i}
< V_i^j
i >
Pisa 07100013
Page 77/123

Wigner distribution is equal to the average value of Wigner operators.
As its continuous counterparts it obeys the following constraints (W.K. Wootters, "Picturing qubits in phase-space", IBM Journal of Research and Development archive Volume 48, Issue 1 (January 2004), quant-ph/0406032 (2004)):
(a) Translational invariance: $W_{(i_1,i_2)} = (V_{i_1}^{i_2})^{\dagger} W_{(0,0)} V_{i_1}^{i_2}$;
(b) The sum of the d^2 Wigner amplitudes $Tr.\rho.W_{(i_1,i_2)}$ is normalized to unity;
(c) Marginals: if we consider STRAIGHT LINES in phase-space defined by the relations $a \odot_G i_1 = b \odot_G i_2 \oplus_G c$, with a b and c elements of the finite (Galois) field with d elements, the averages of Wigner operators along such lines (marginals) are equal to a projector onto one of the MUB's states.
Moreover, marginals along non-intersecting parallel lines correspond to projectors onto orthogonal states of a same MUB while marginals taken along non-parallel directions correspond to projectors onto states from different MUB's.

Appendix: Epistemic interpretation

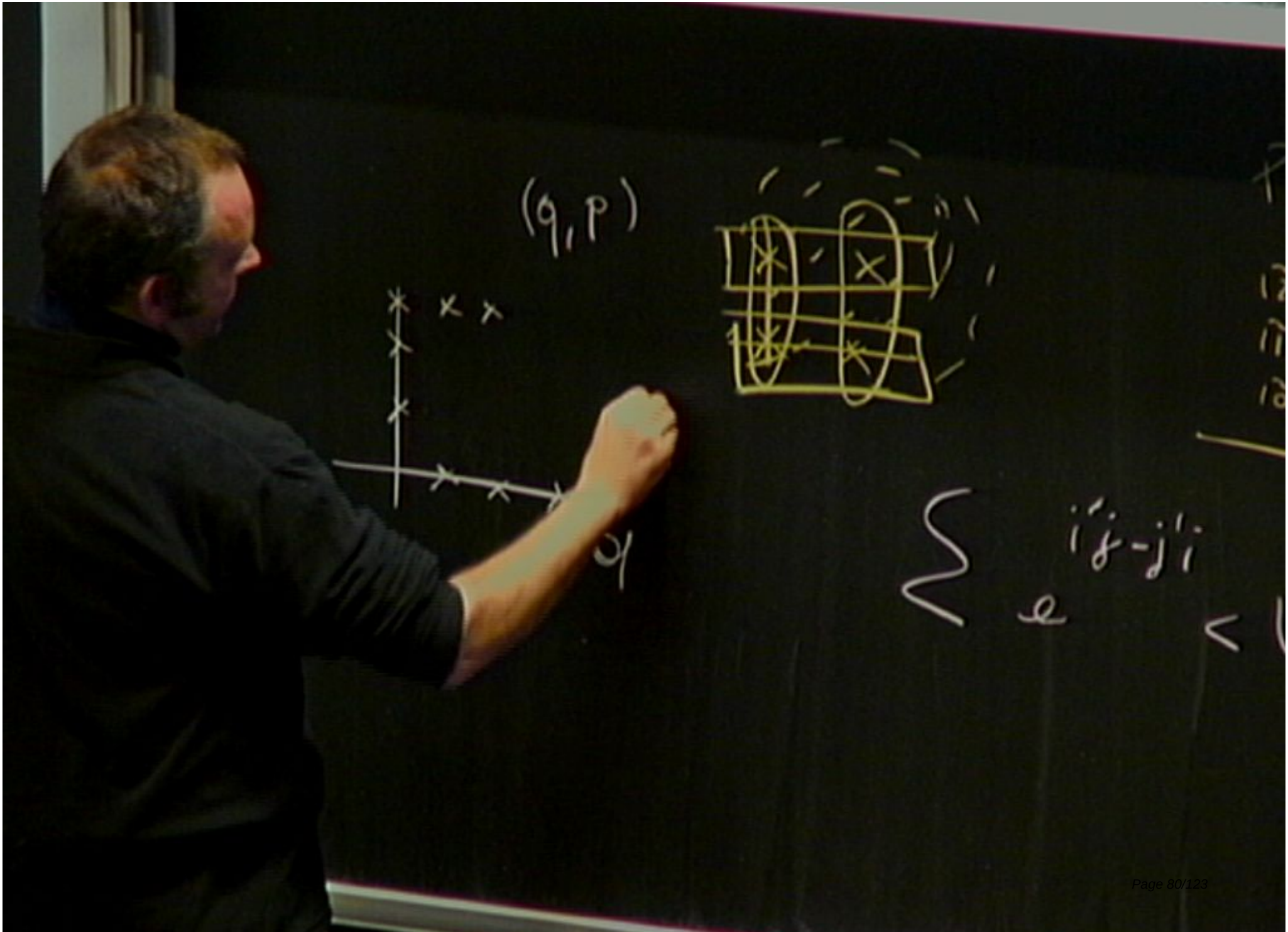
and the role of dimensions.

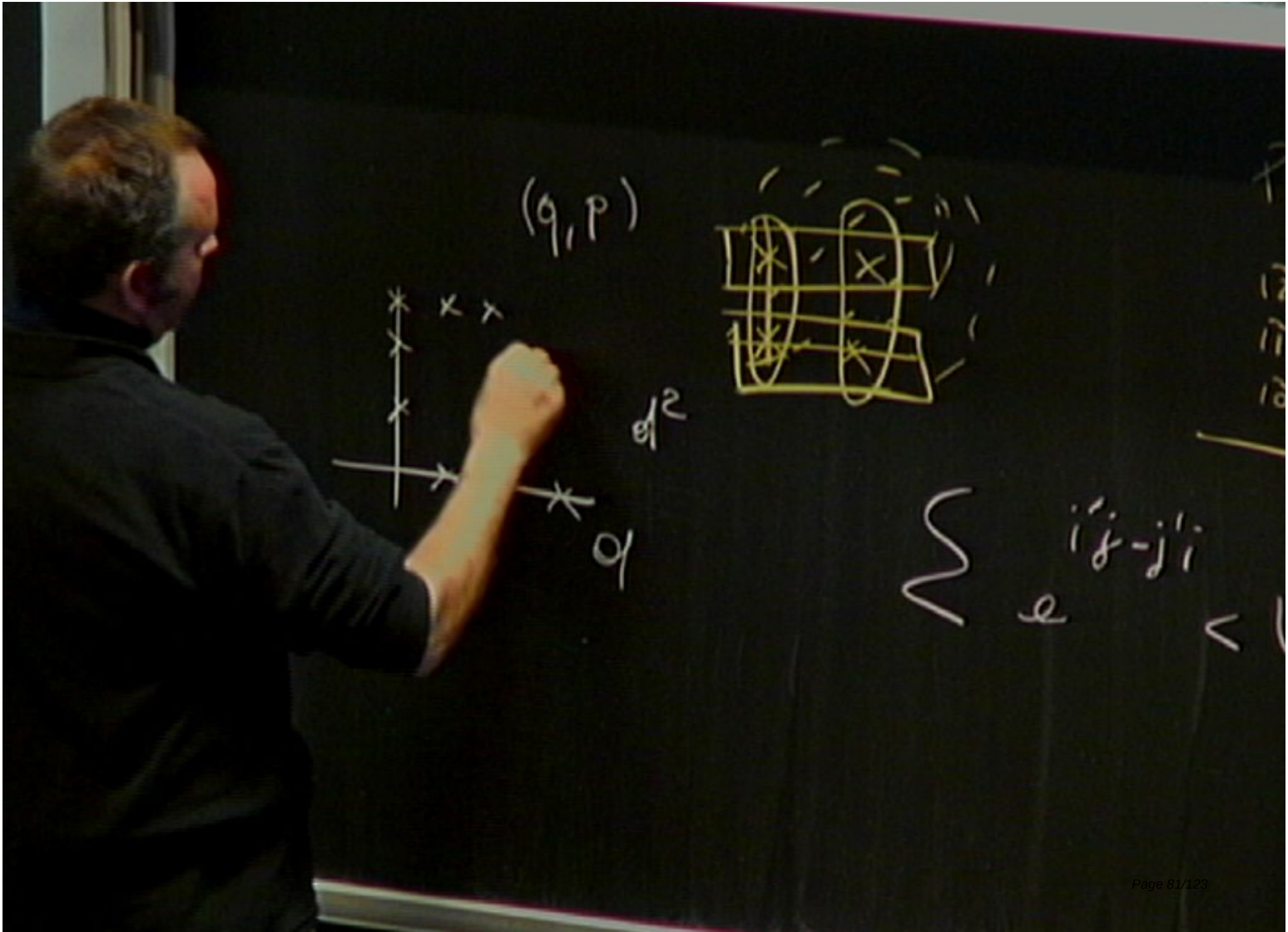
-The labels of the Wigner operators form a d times d square that plays the role of a discrete phase space.

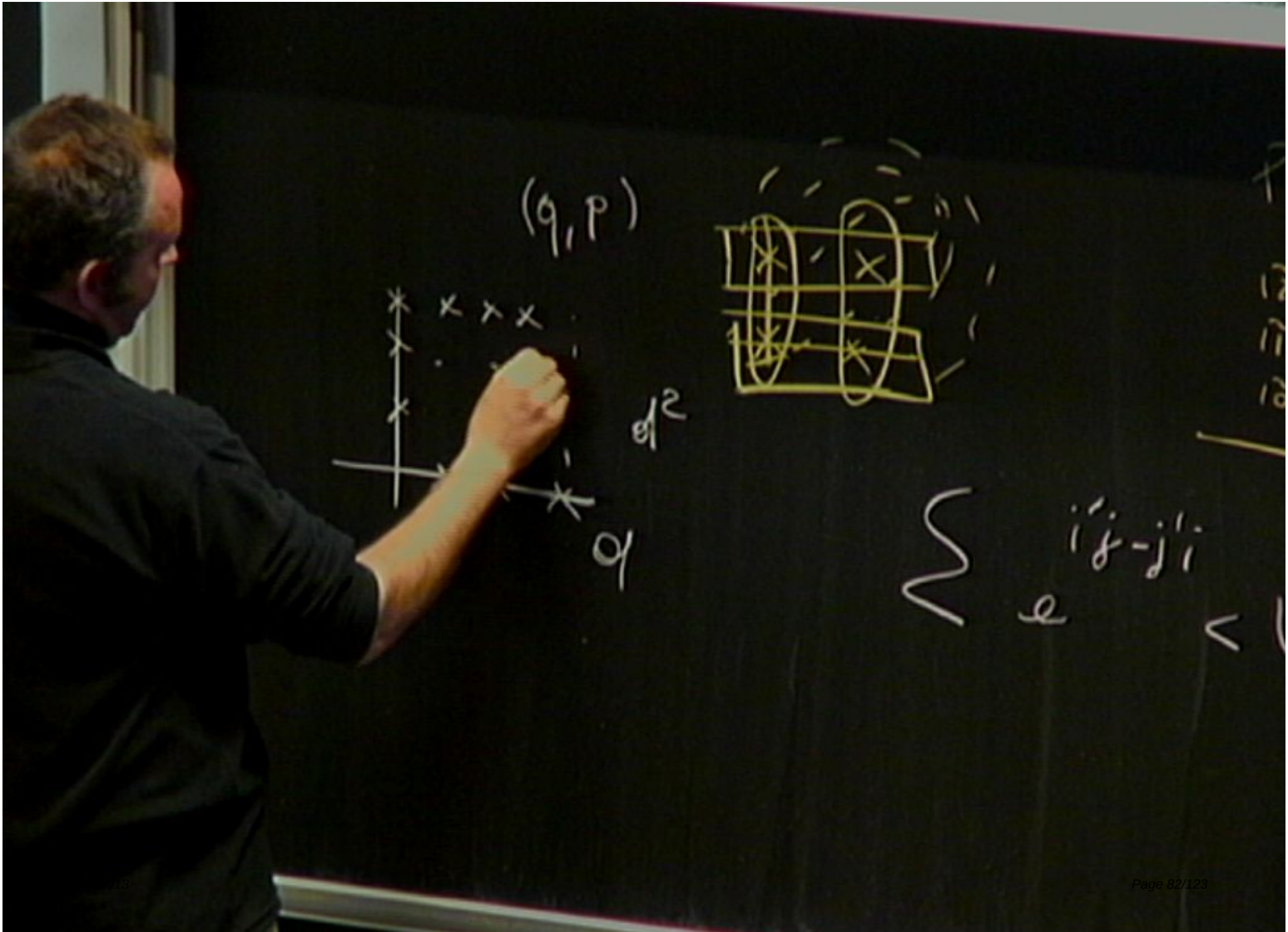
-The horizontal and the vertical axes correspond to a discrete version of the position-impulsion representations.

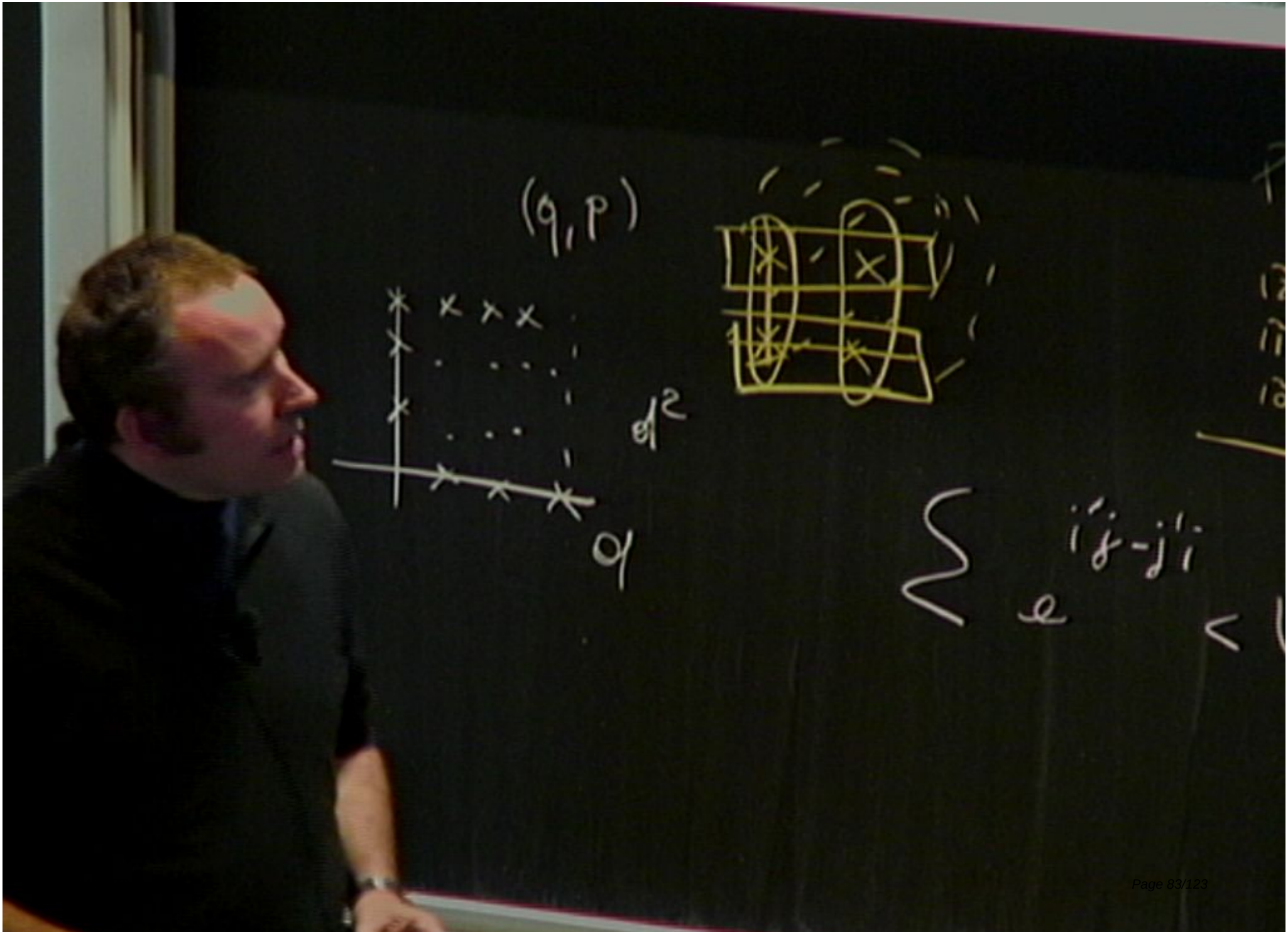
-Then, in virtue of the marginal property, we have that each vertical line of the square (there are d of them) corresponds to a state of the computational basis, each horizontal line corresponds to a state of the dual (Galois-Fourier) basis and more generally each set of parallel straight lines corresponds to a state of one of the MUB's.

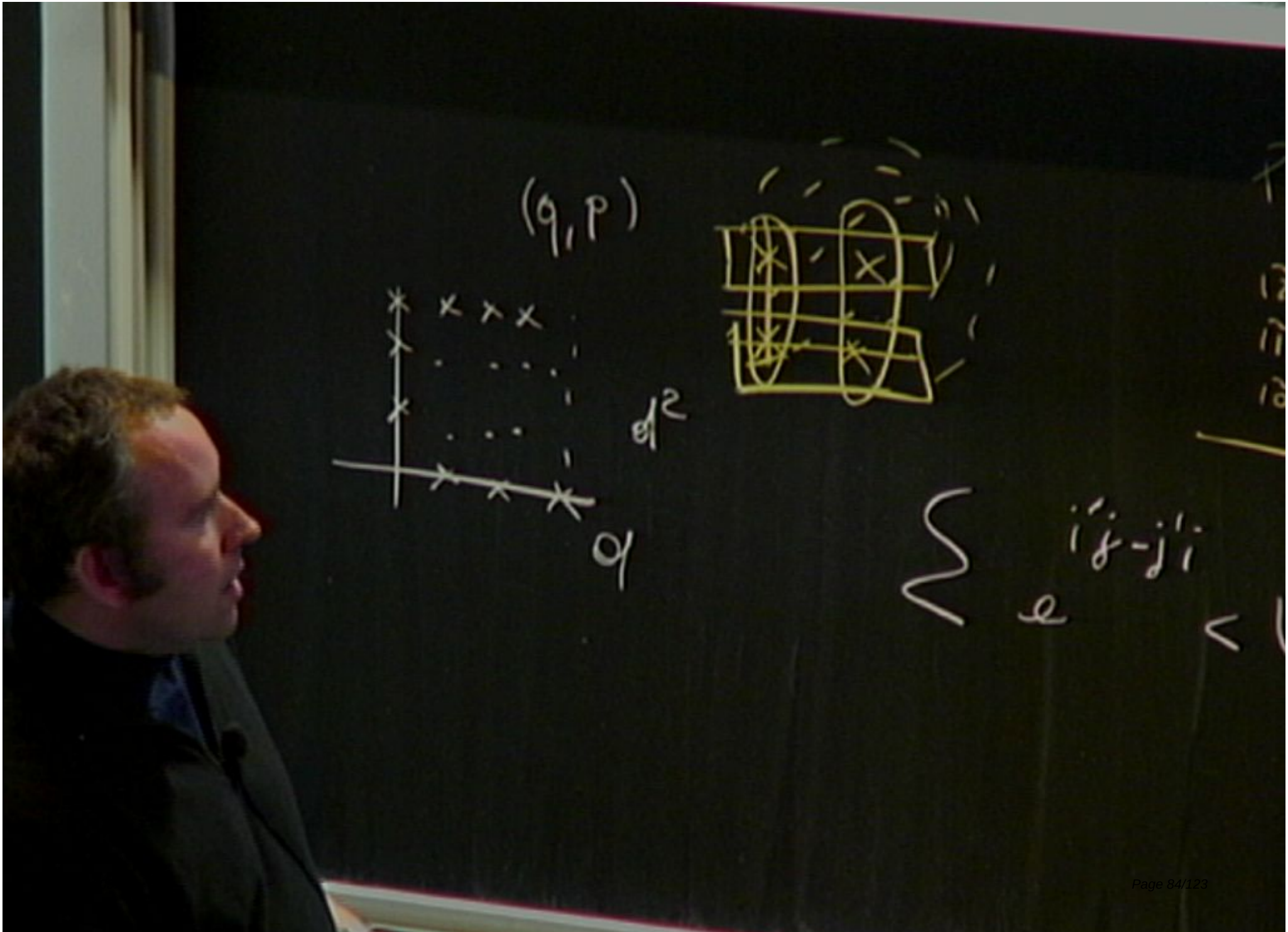
-This property agrees with the fact that when the Mean King prepares such a state d detectors among d^2 detectors are likely to fire, with the same probability, which reflects a complementary relation between pairs of MUB's.

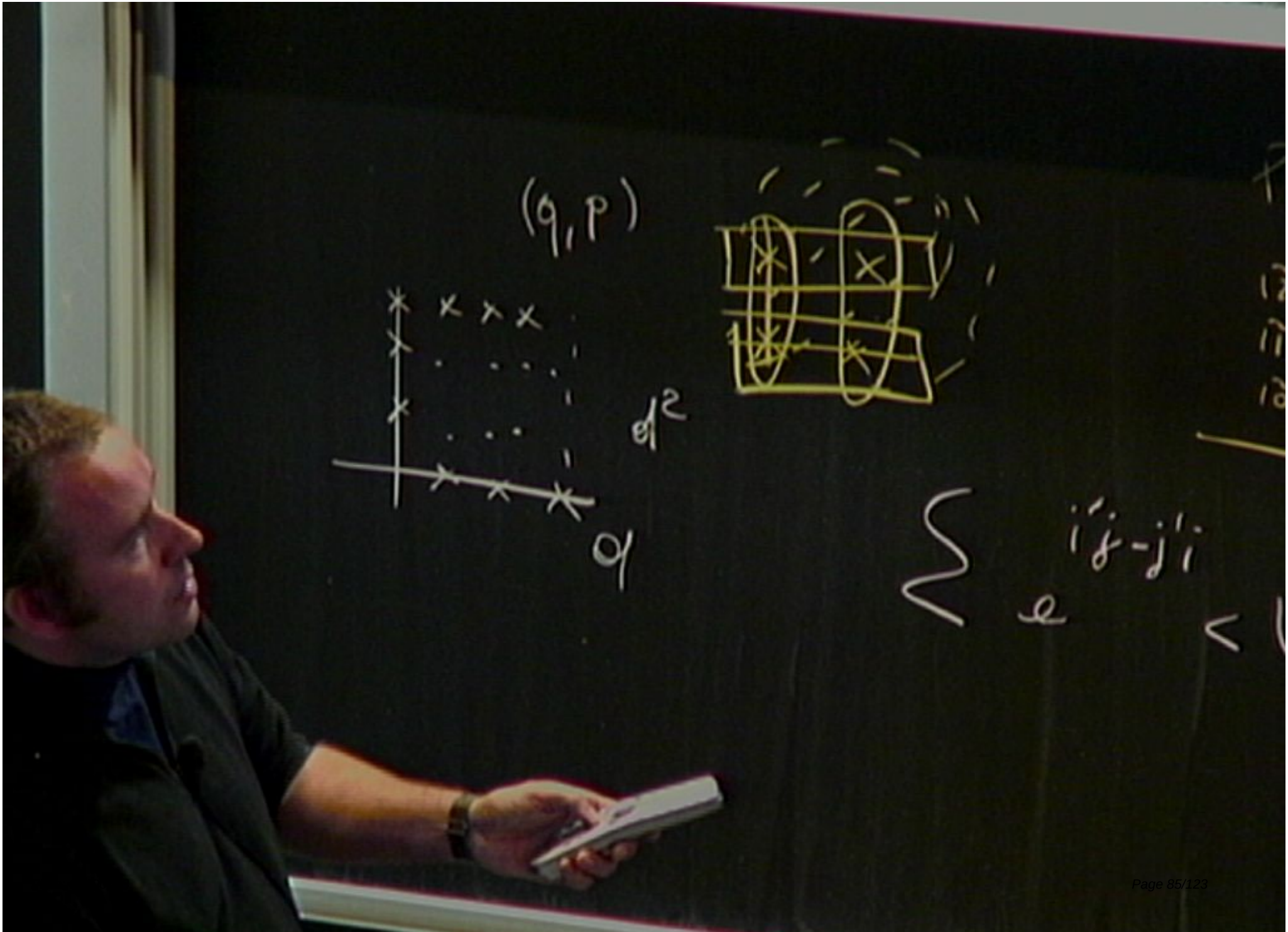

(q, p)
q
$\sum e^{i\vec{i}-\vec{j}i}$

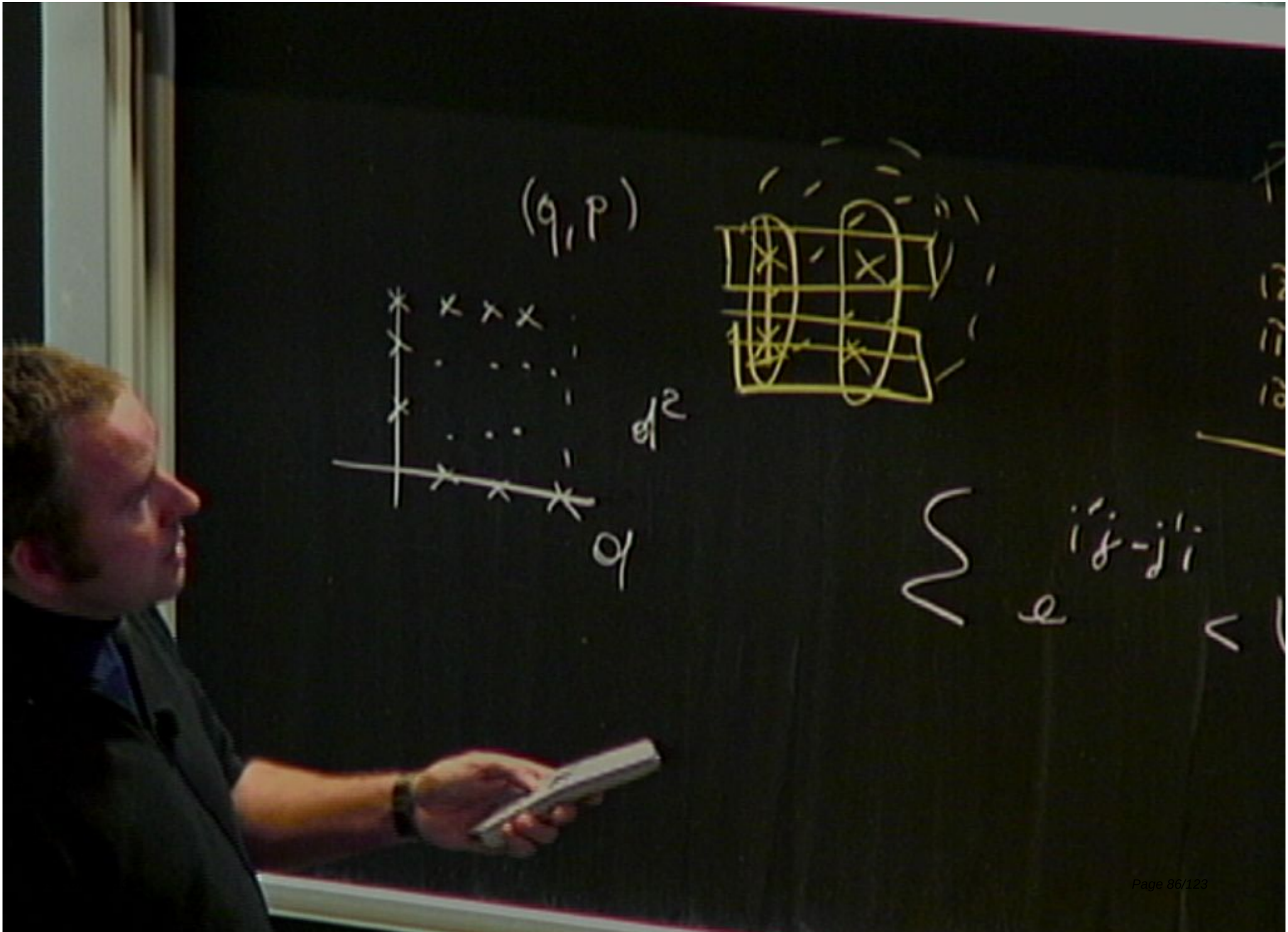

(q, p)
d²
q
Σ
e
i'i-j'i
<

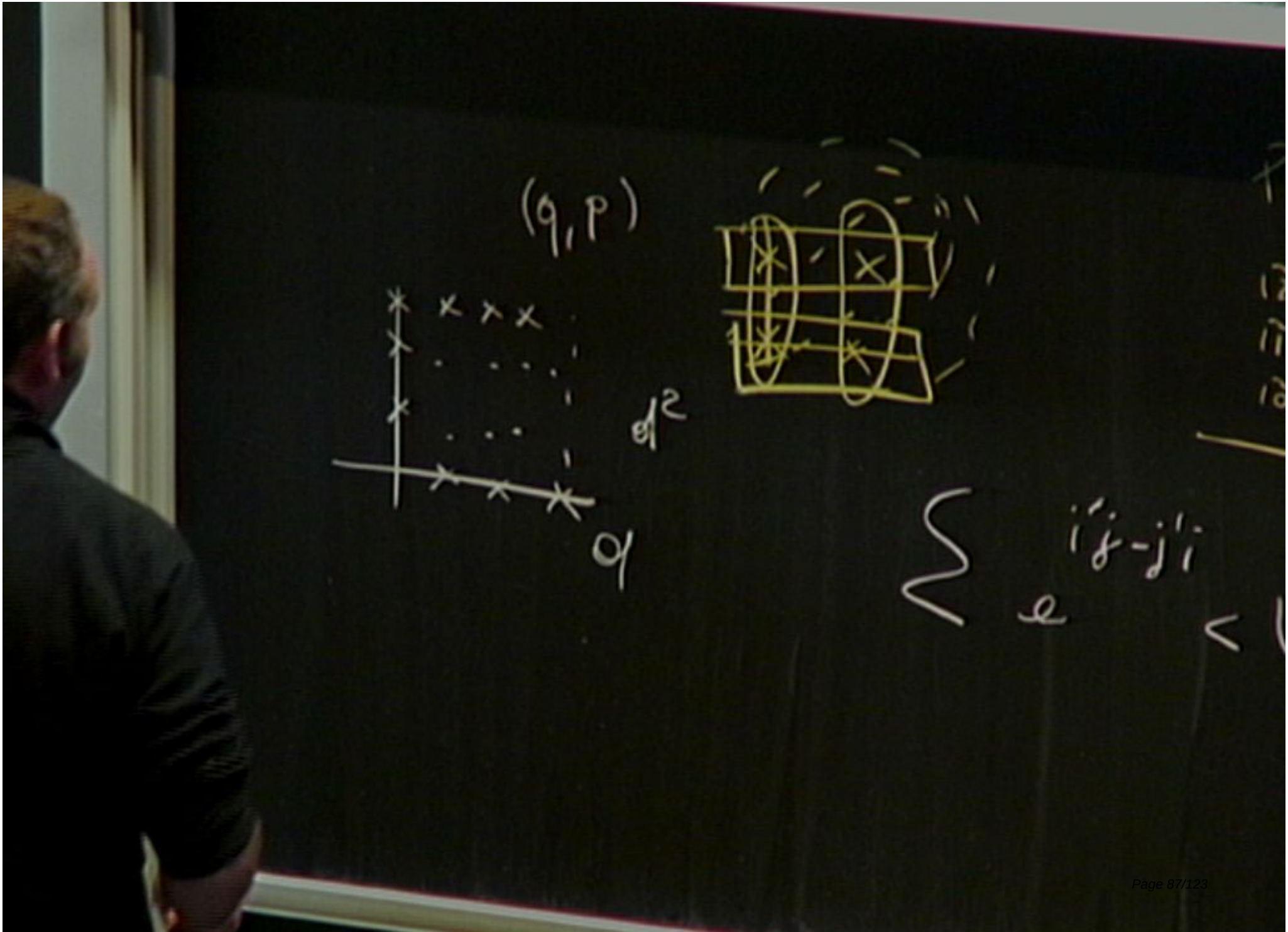

(q, p)
d²
q

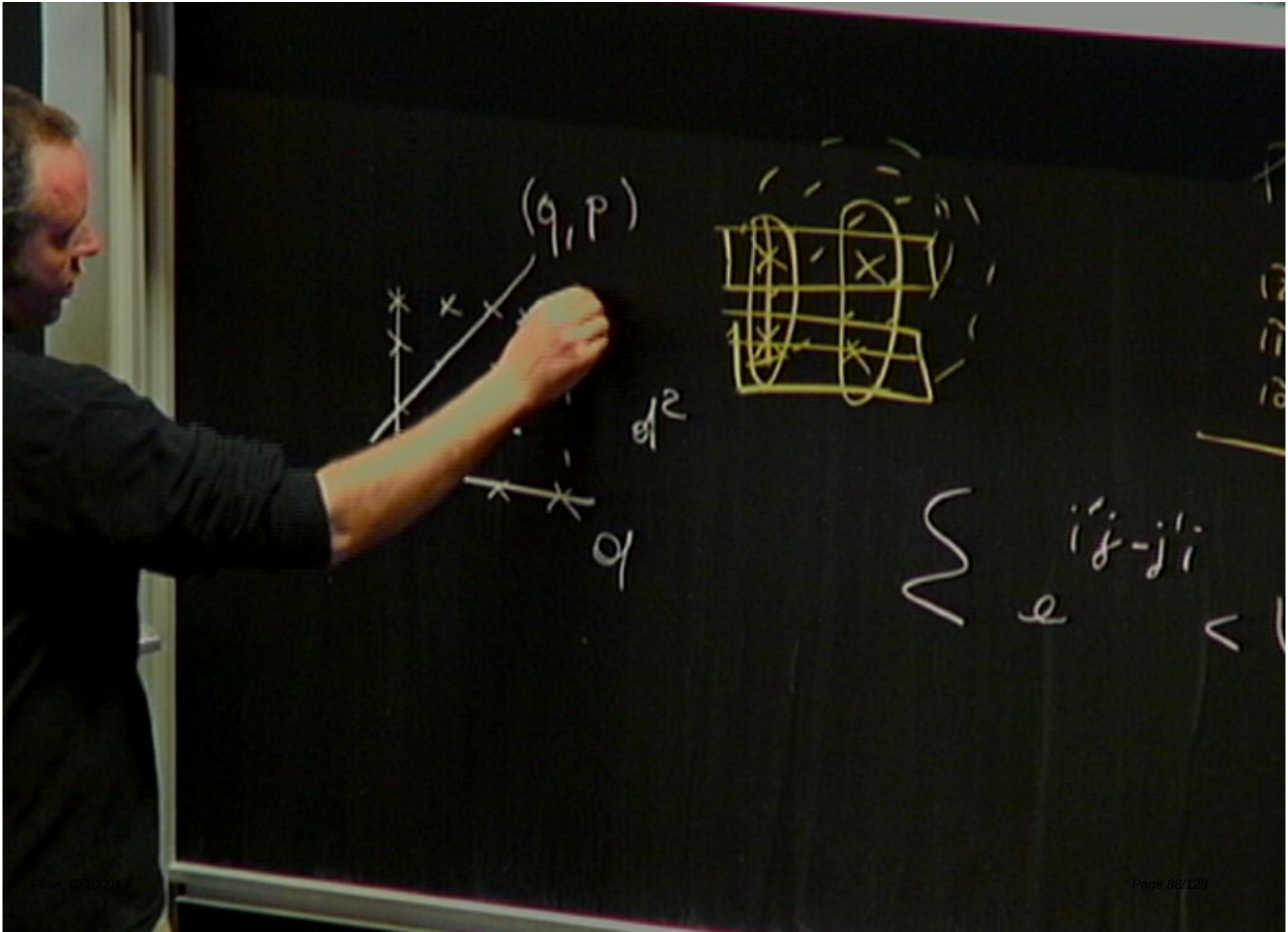

(q, p)
d^2
q
$\sum e^{i'j-j'i}$

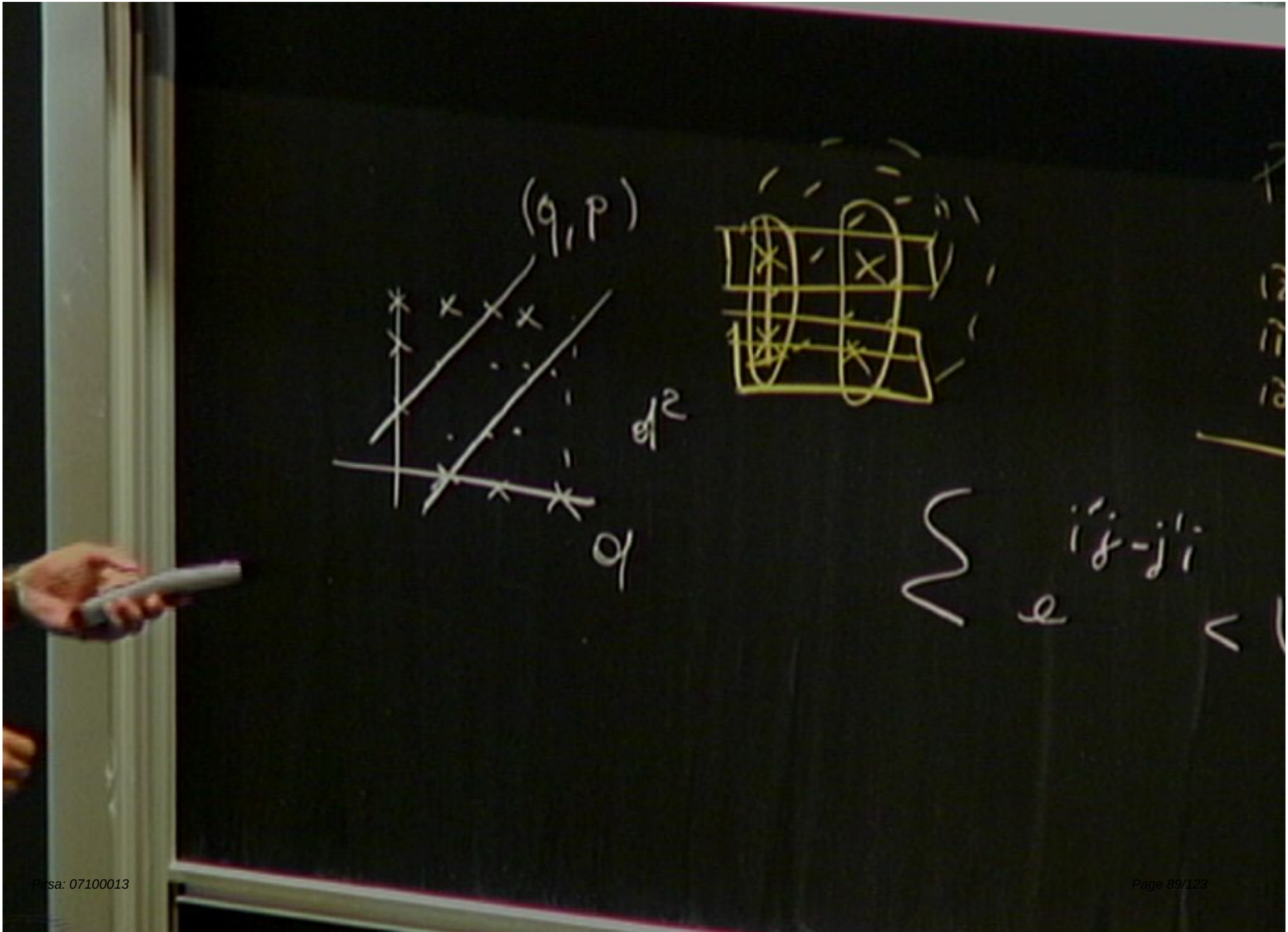

(q, p)
d²
q
Σ
e
i'i-j'i
<

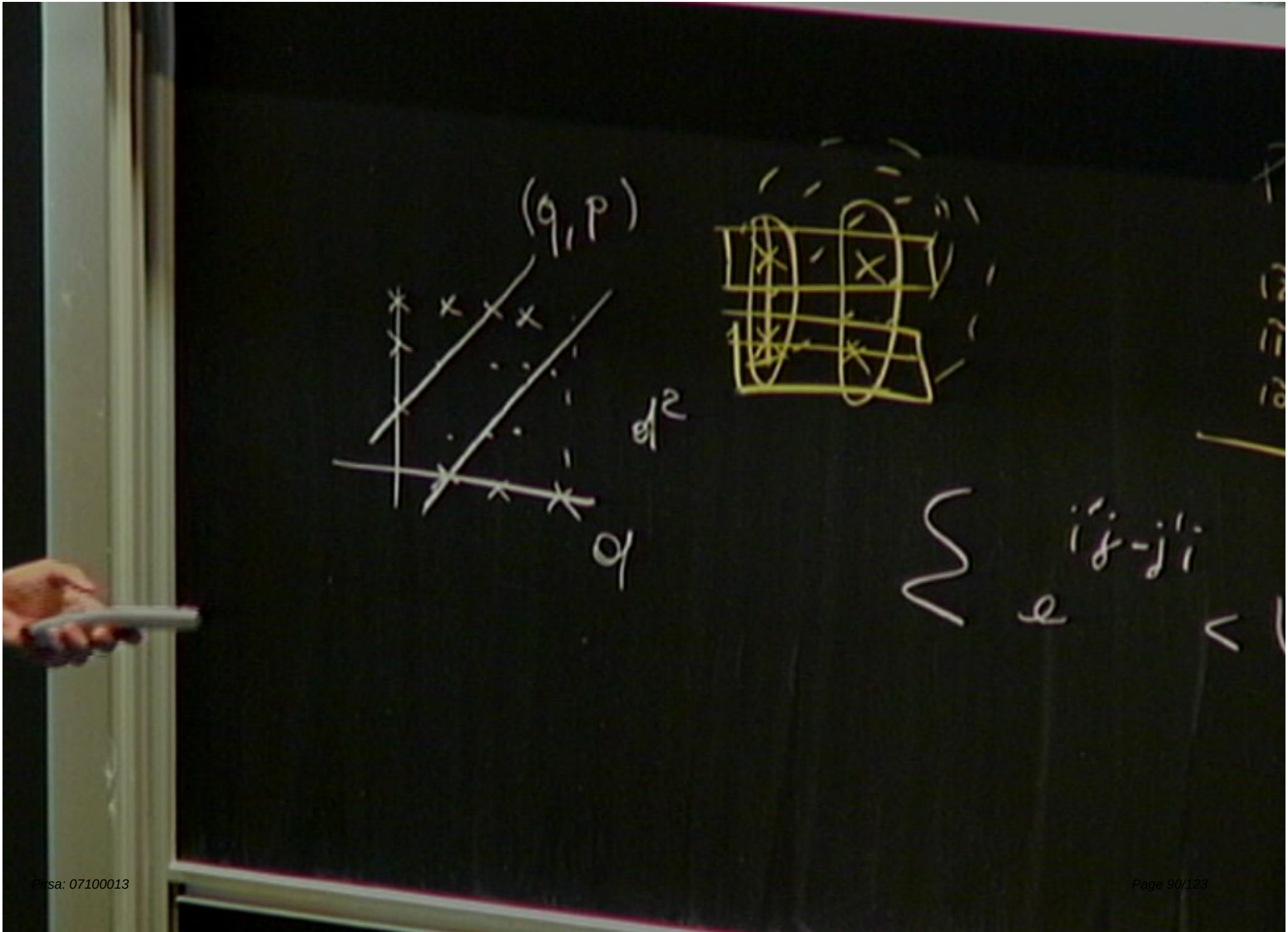

(q, p)
d²
q
Σ
e
i'i-j'i

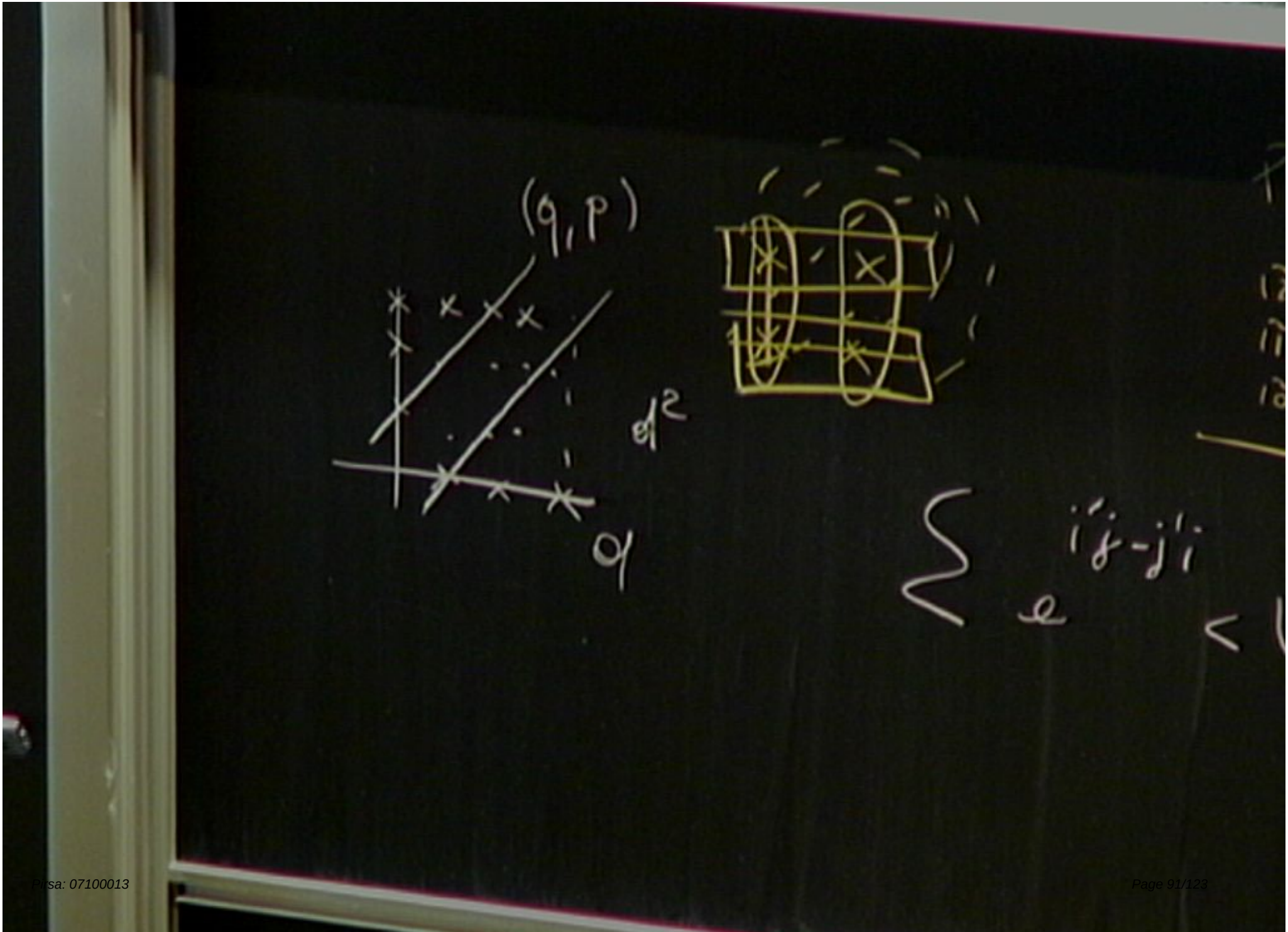

(q, p)
d^2
q
$\sum e^{i'j-j'i}$

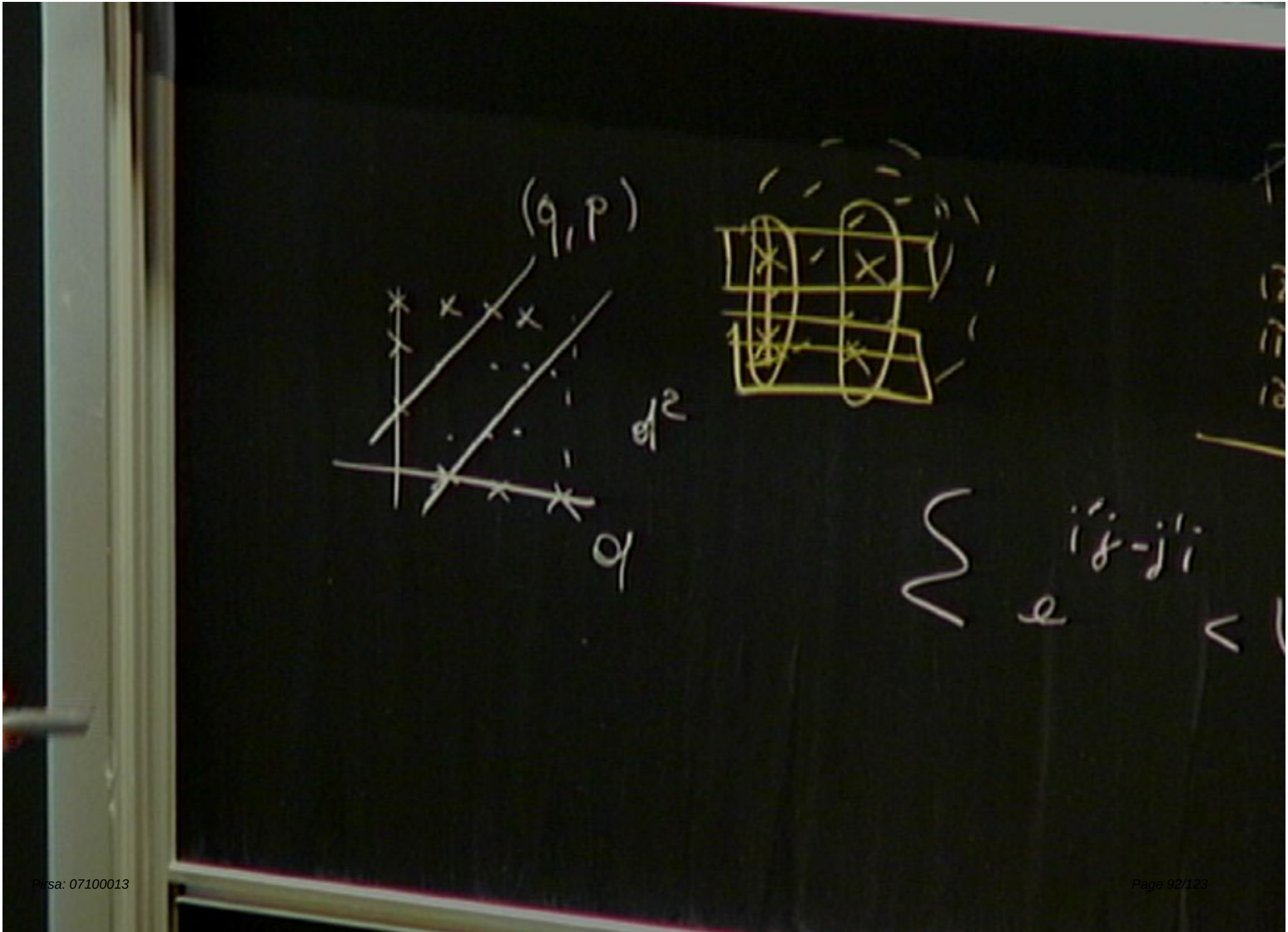

(q, p)
q
$\sum e^{i\vec{j}-\vec{j}'i}$

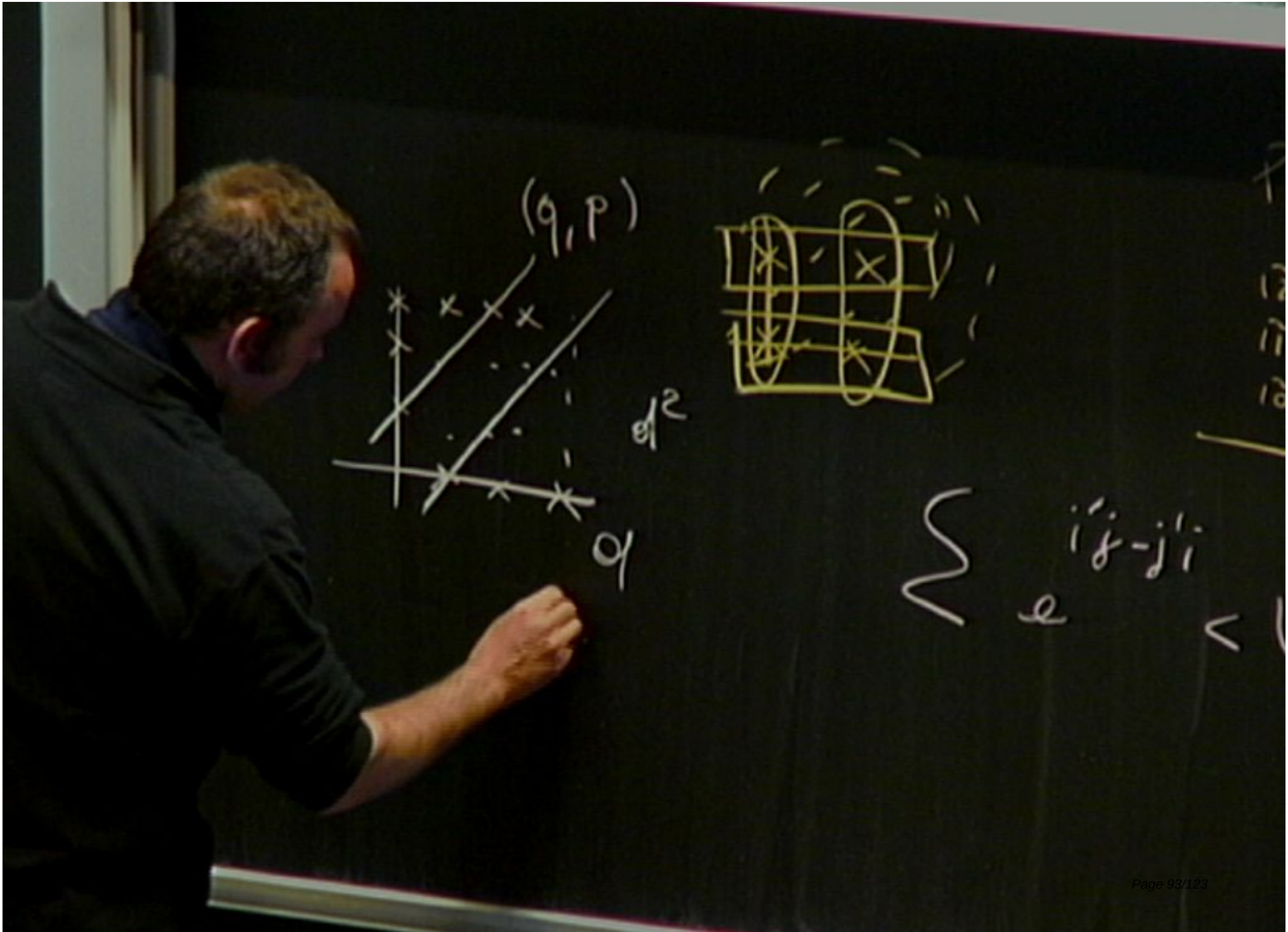

(q, p)
d²
q
Σ
e
i'j - j'i
< 1

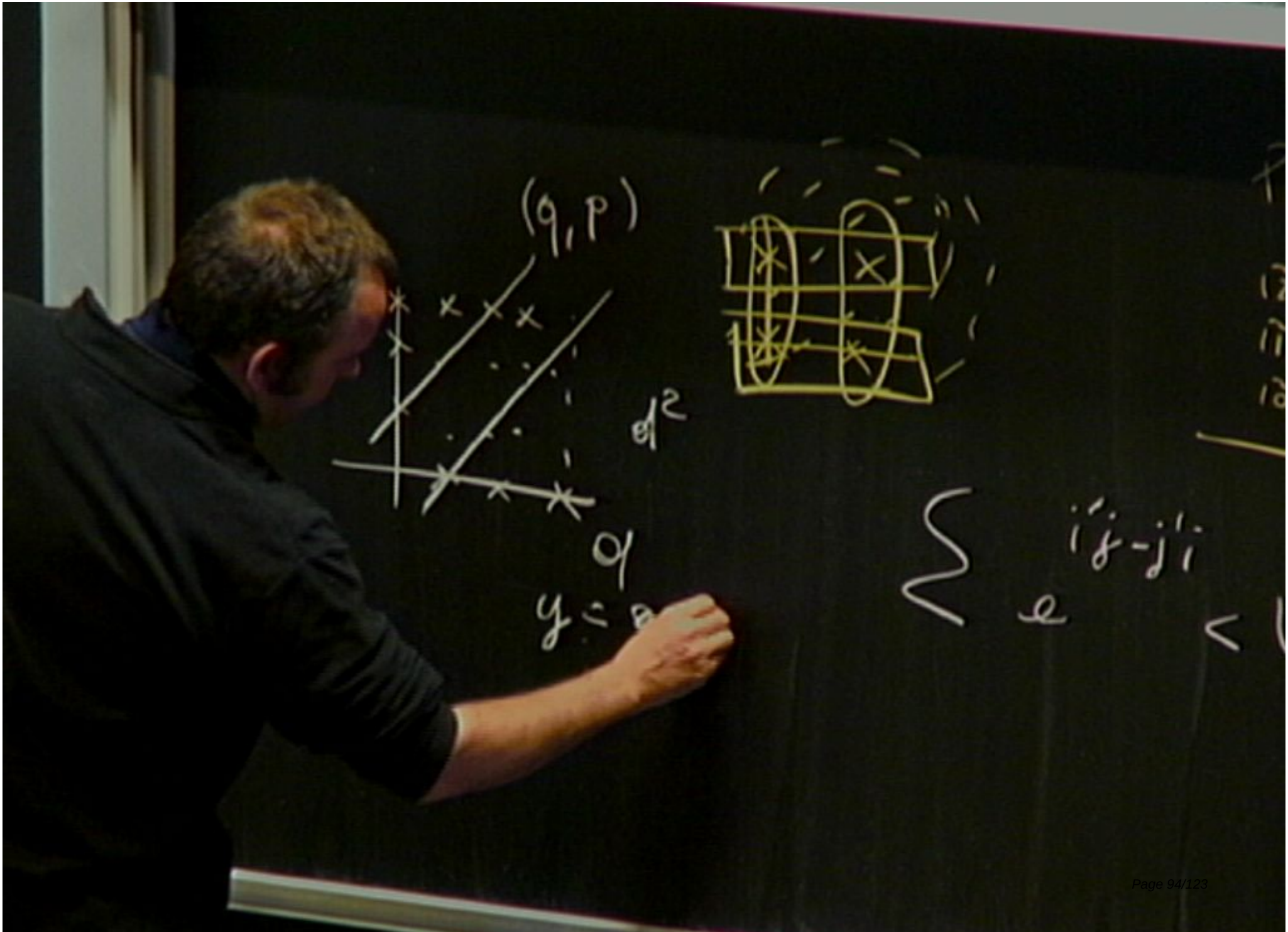

(q, p)
d²
q
Σ
e
i'j-j'i
<

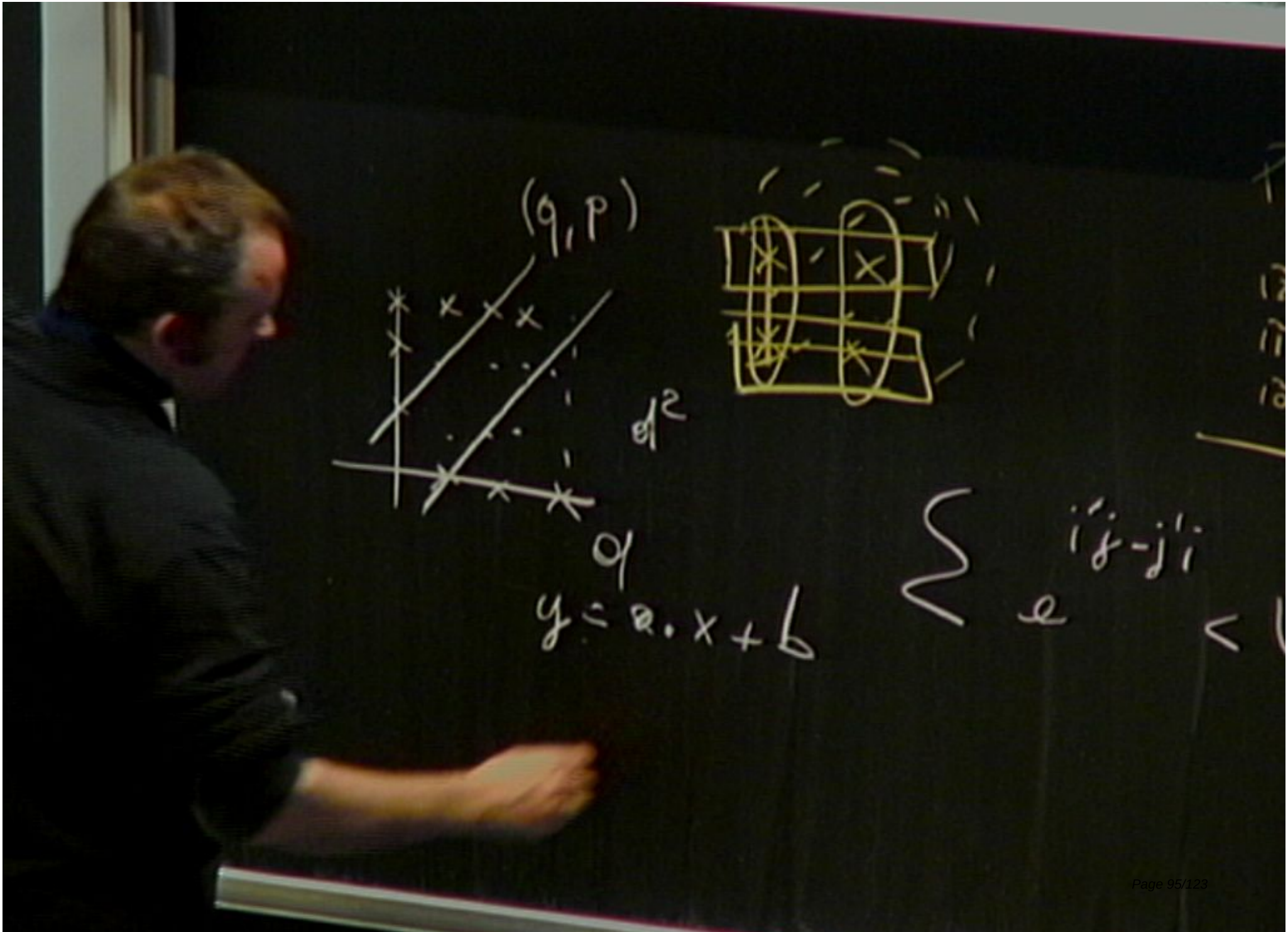

(q, p)
d²
q
Σ
e
i'j-j'i
<

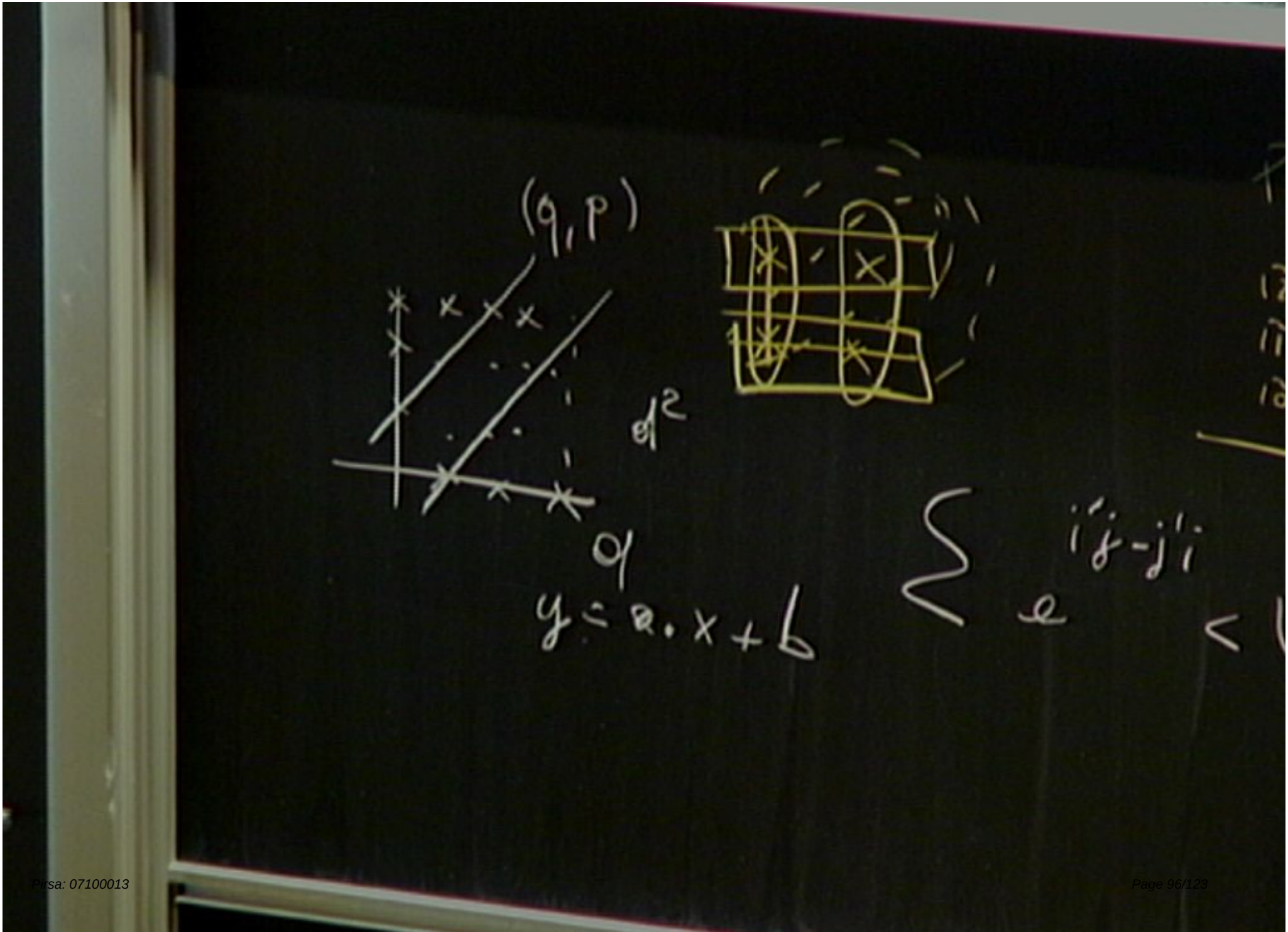

(q, p)
d^2
q
$\sum e^{i\vec{j}-\vec{j}'i}$

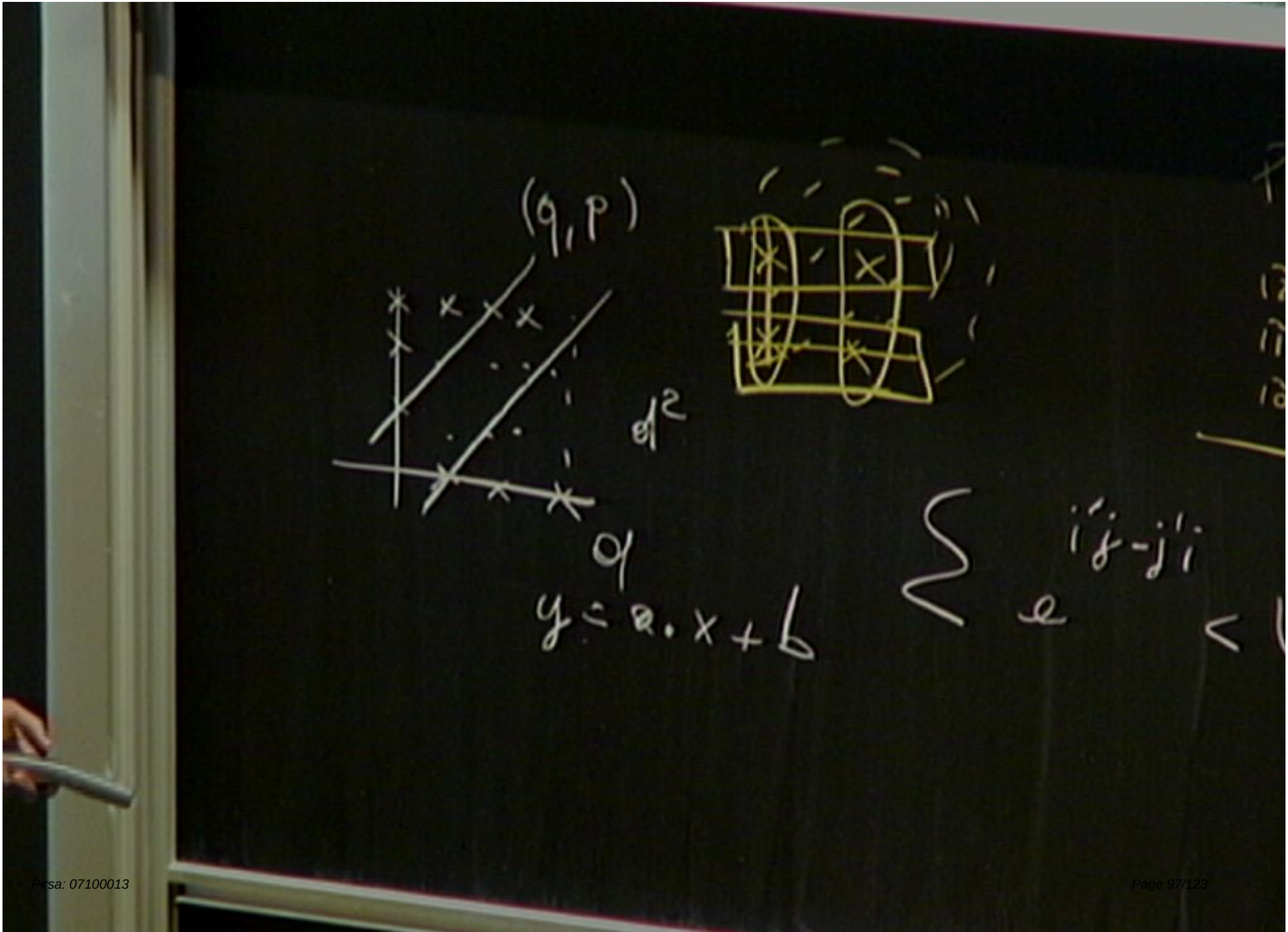

(q, p)
d²
q
Σ e^{i'i-j'i}

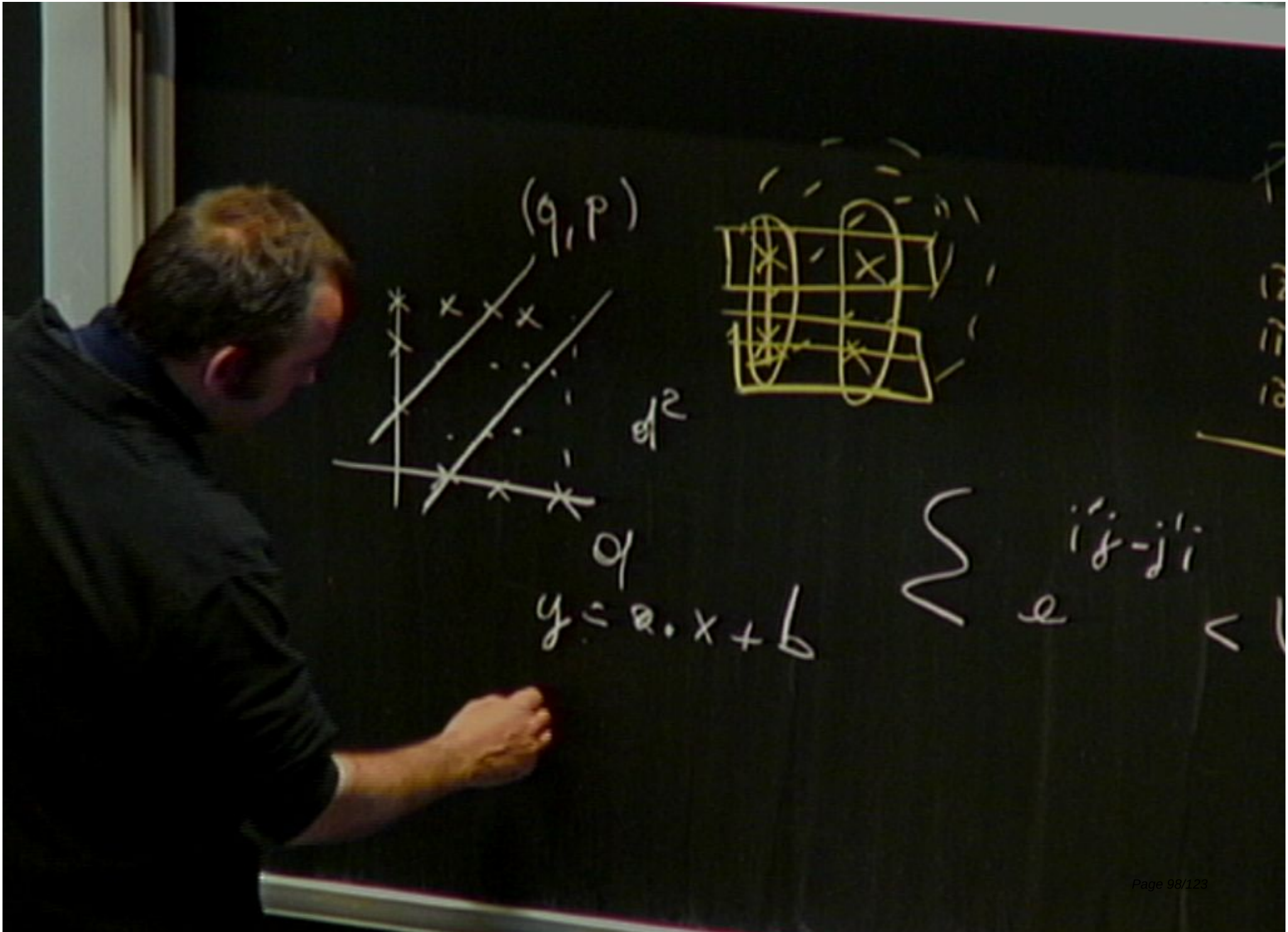

(q, p)
d²
q
Σ
e
i'j-j'i
<

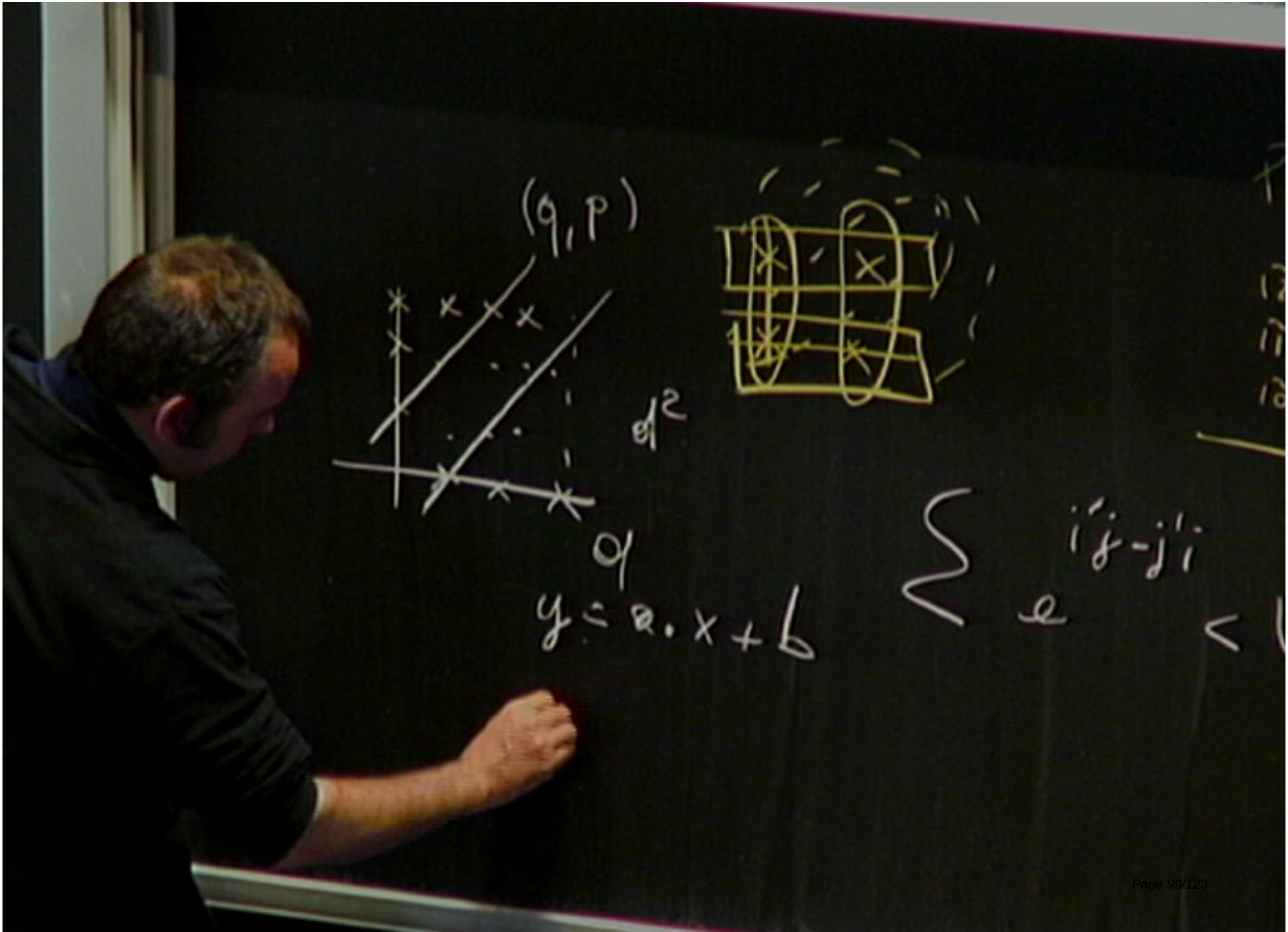

(q, p)
d^2
q
$y = a$
$\sum e^{i\,i-j\,i}$

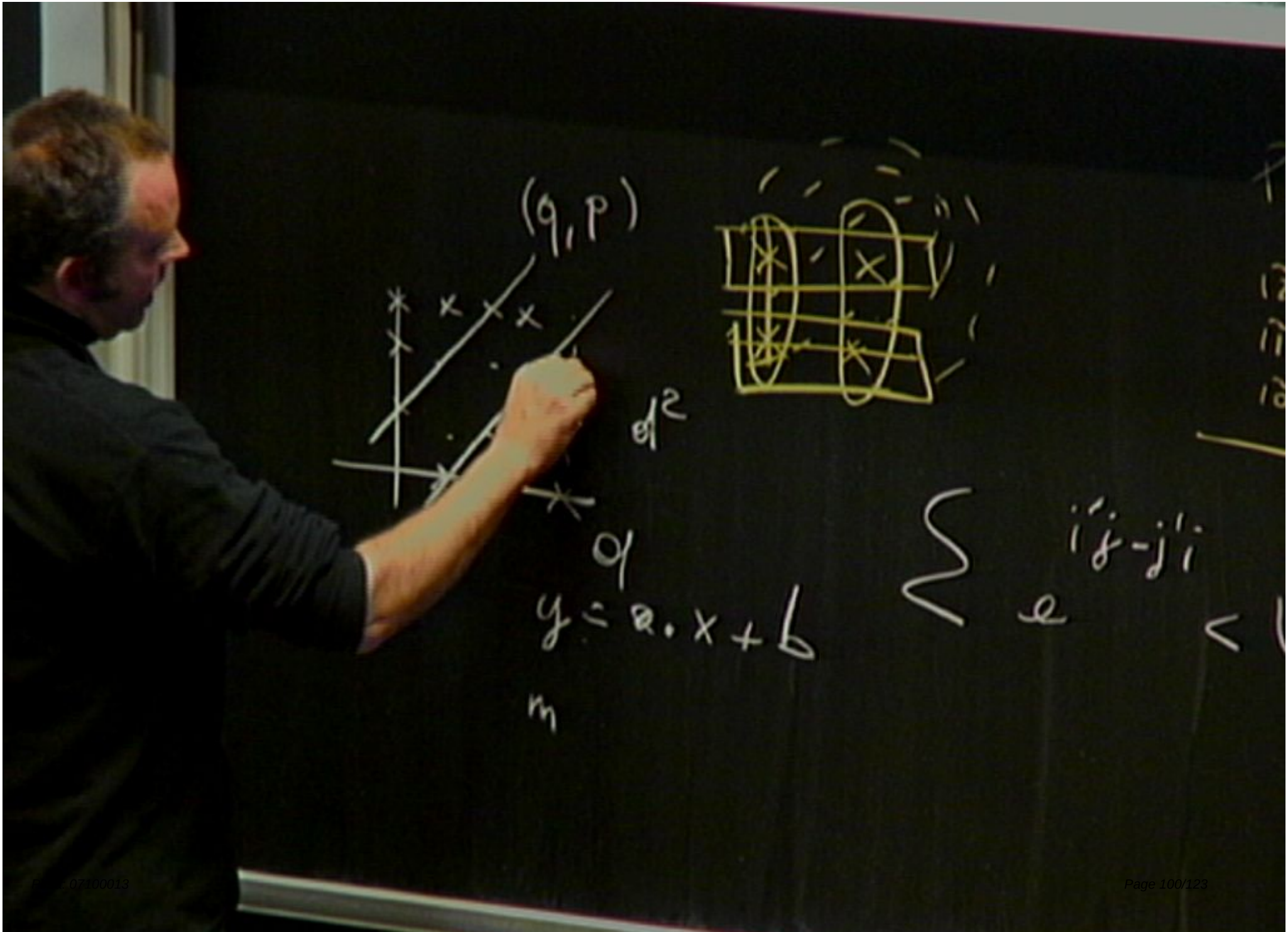

(q, p)
d²
q
y = a · x + b
Σ
e
i'j-j'i

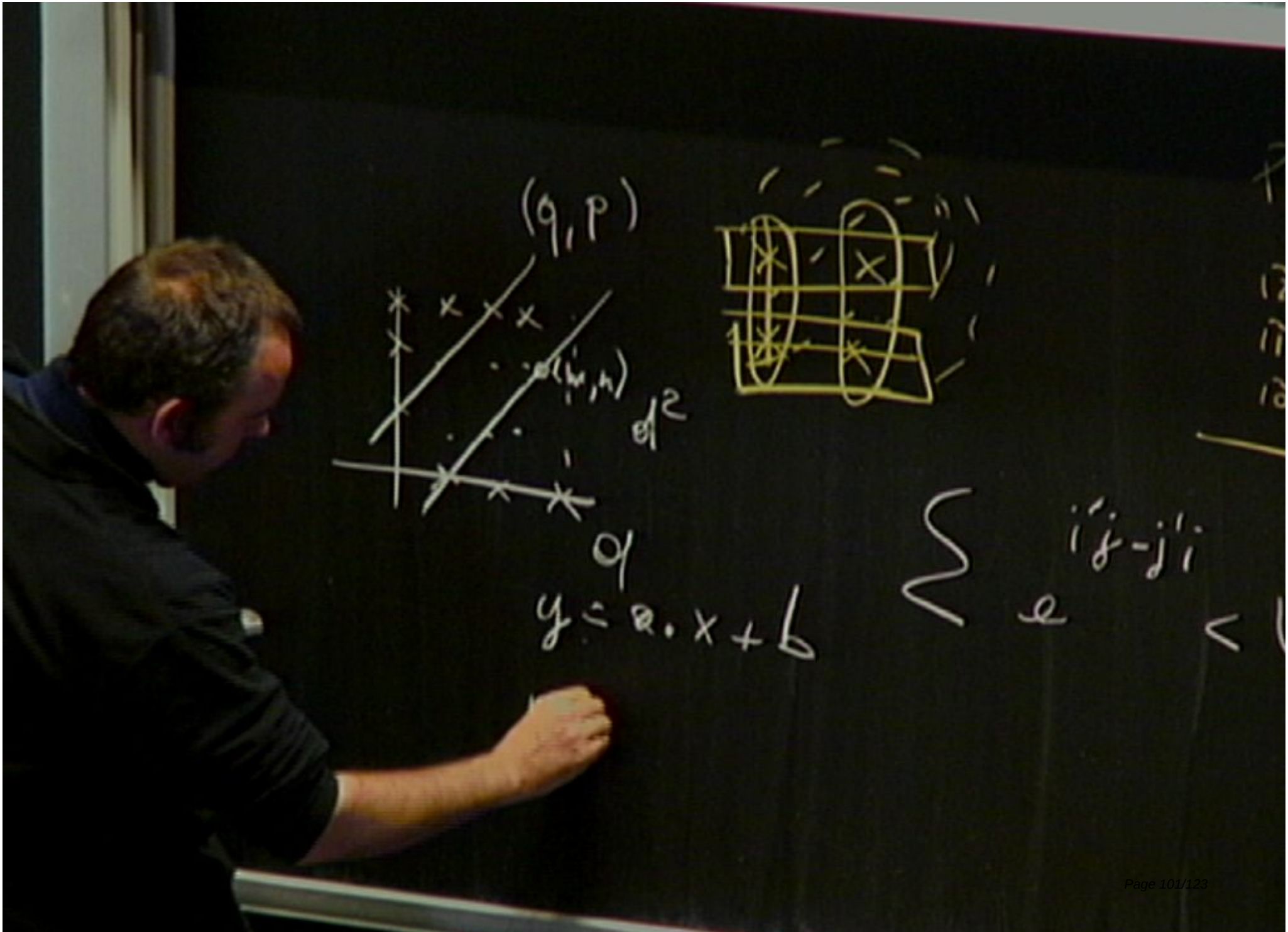

(q, p)
d²
q
y = a · x + b
Σ
e
i'i - j'i

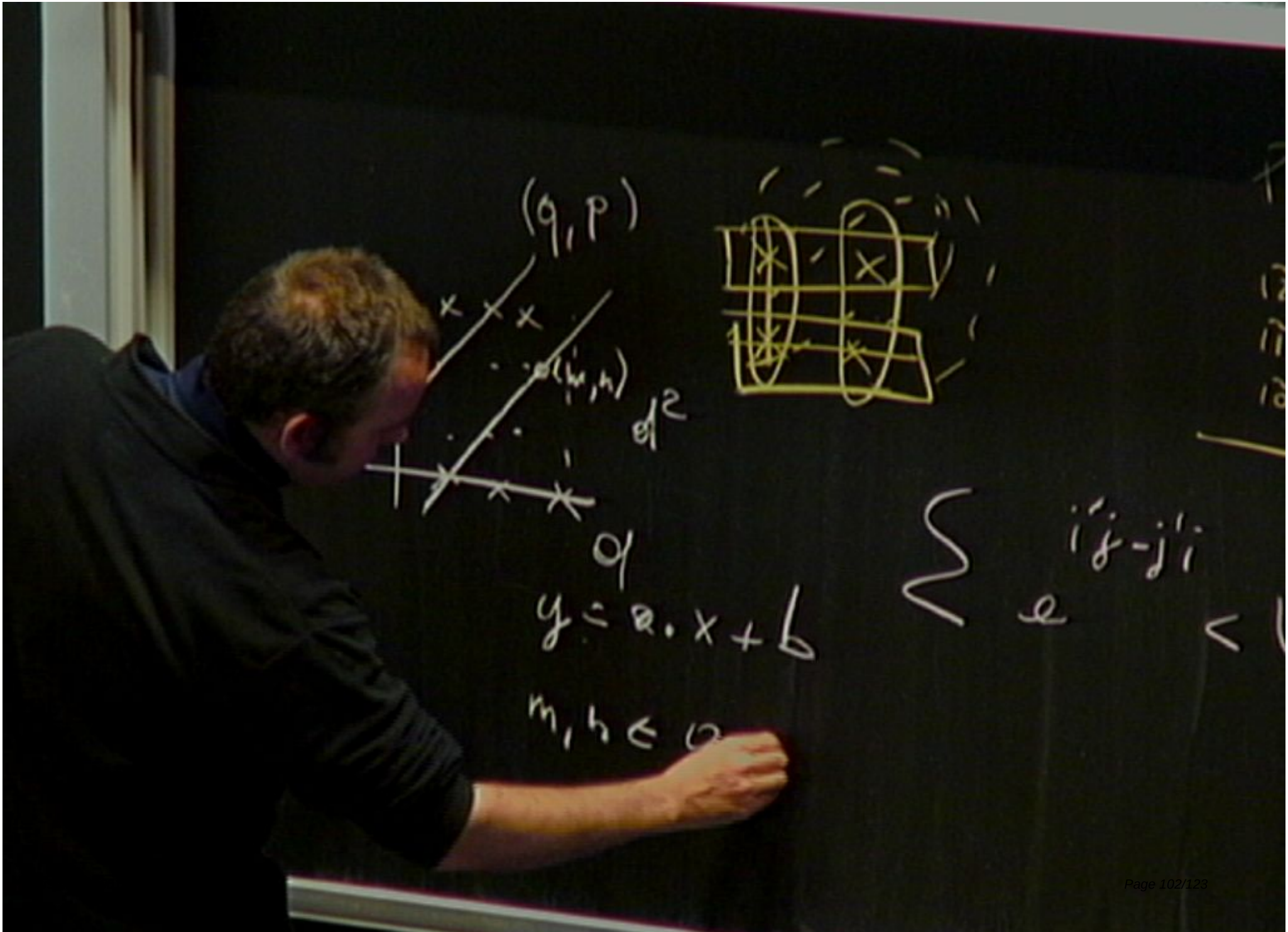

(q, p)
d²
q
y = a · x + b
Σ
e
i'j-j'i

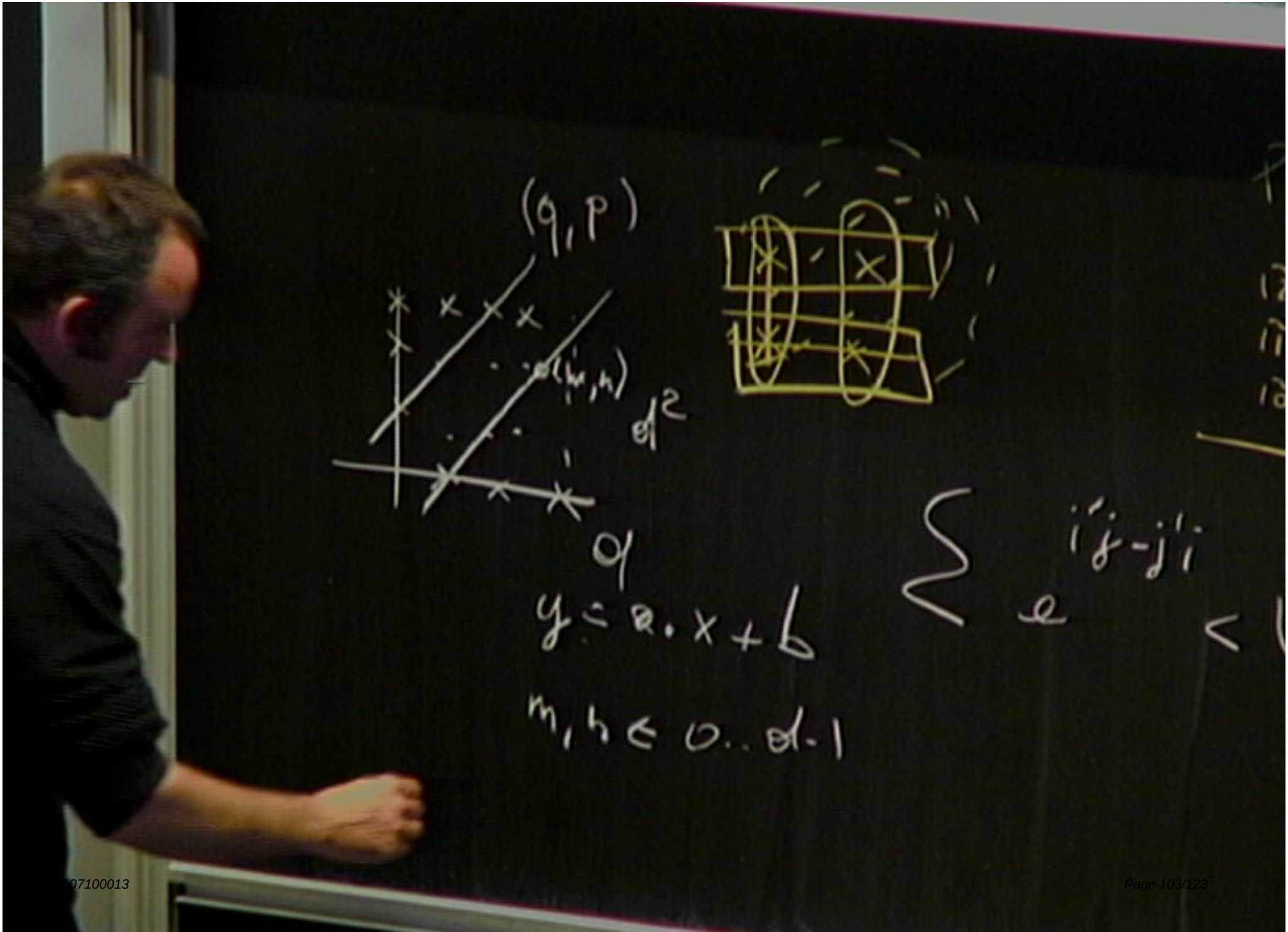

(q, p)
d²
q
y = a · x + b
Σ
e
i'j-j'i

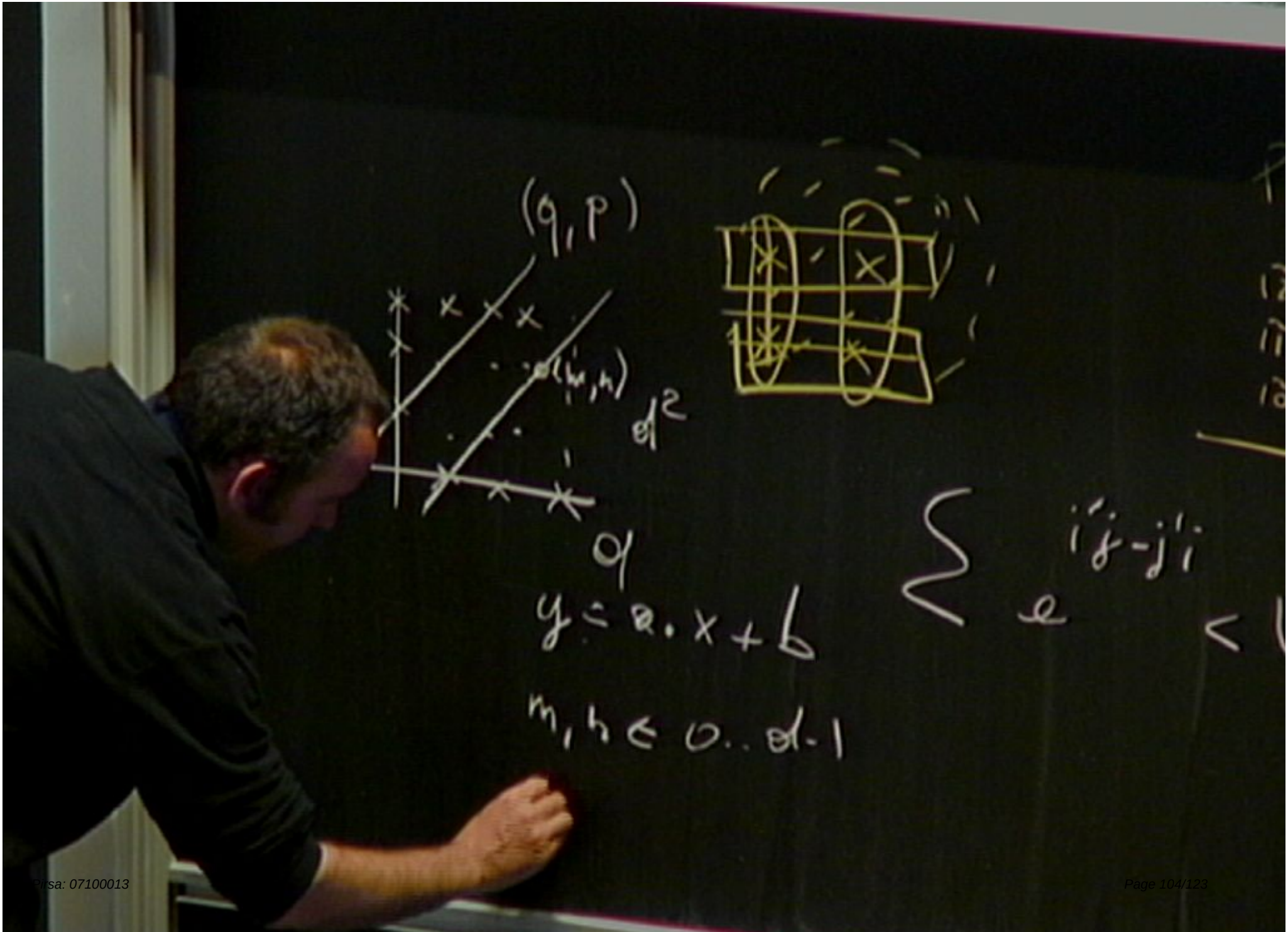

(q, p)
d²
q
y = a · x + b
Σ
e
|i - j|

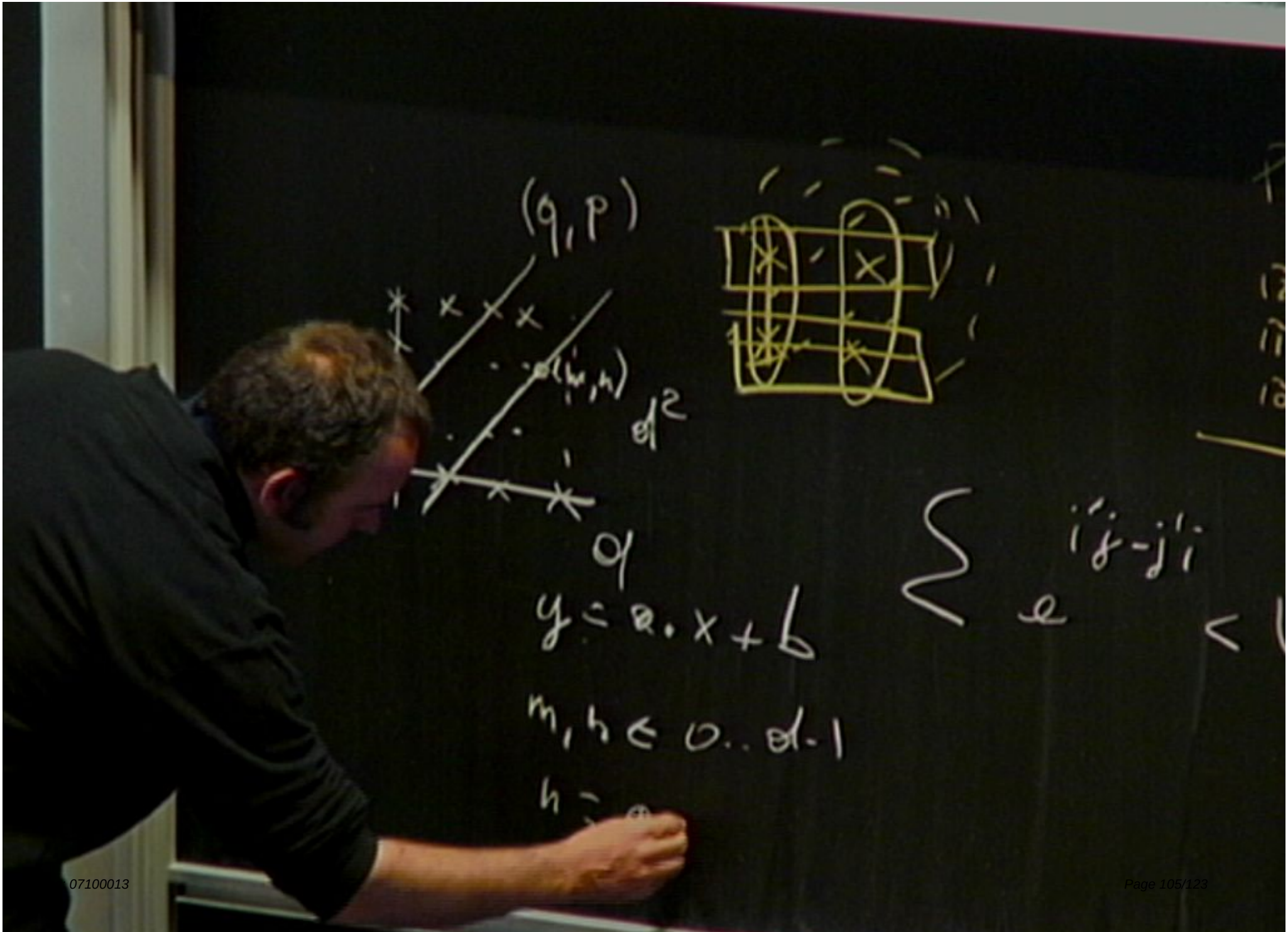

(q, p)
d²
q
y = a · x + b
m
Σ
e
i'j-j'i
<

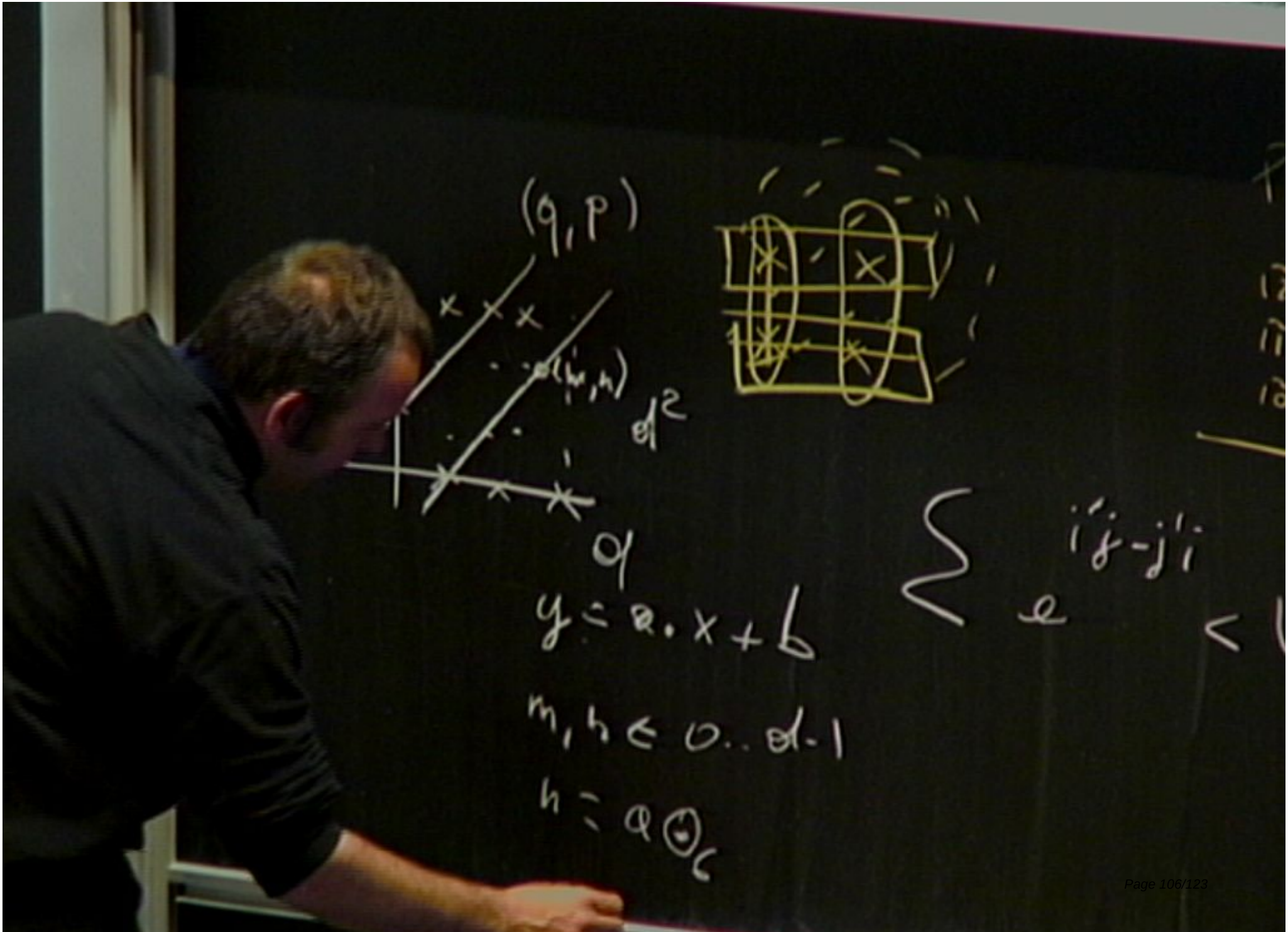

(q, p)
d²
q
y = a · x + b

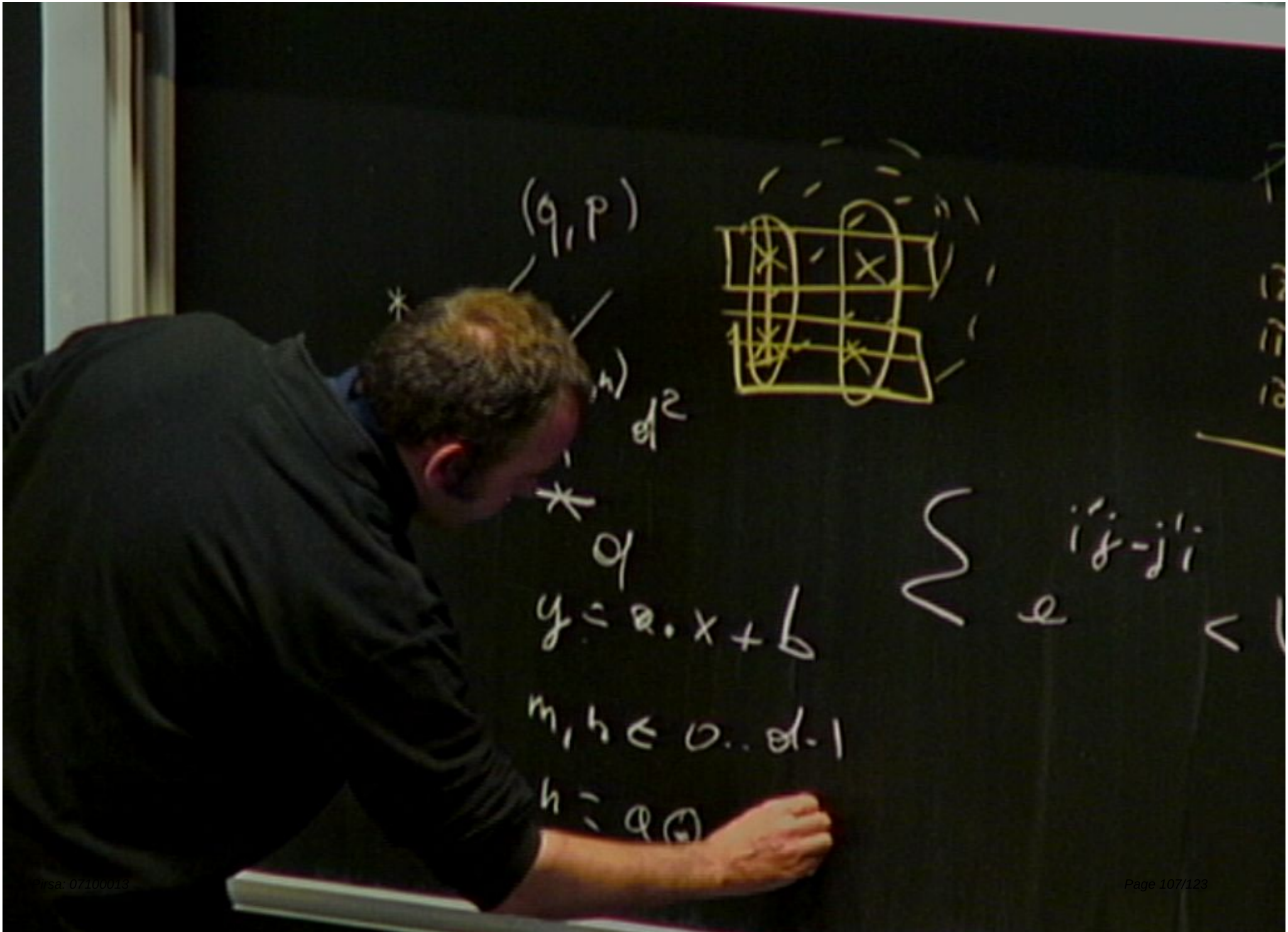

(q, p)
(m, n)
d²
q
y = a · x + b
m, n ∈ ℤ
Σ
e
i'i-j'i

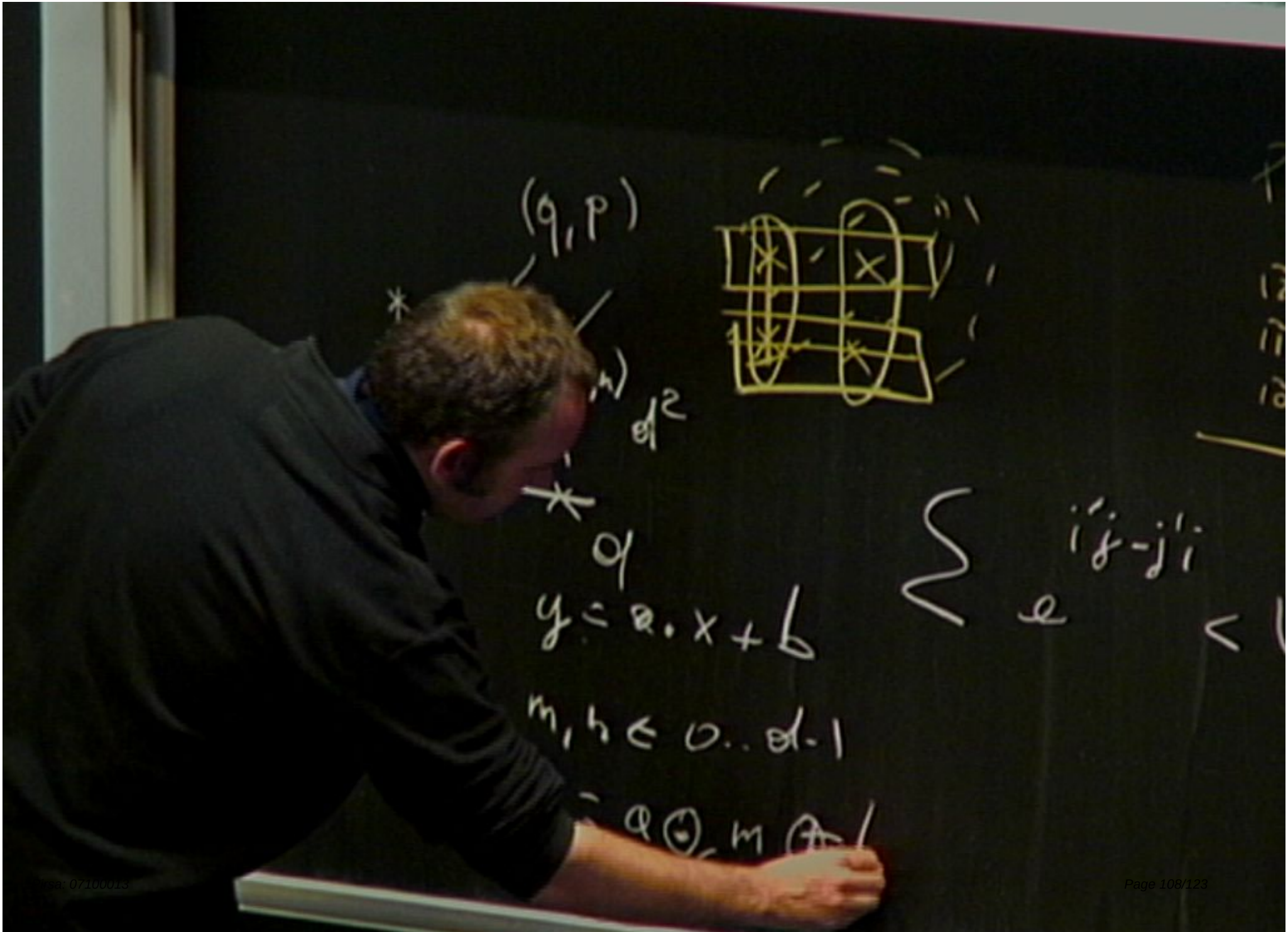

(q, p)
d^2
q
y = a · x + b
m, n ∈ 0 .. d-1

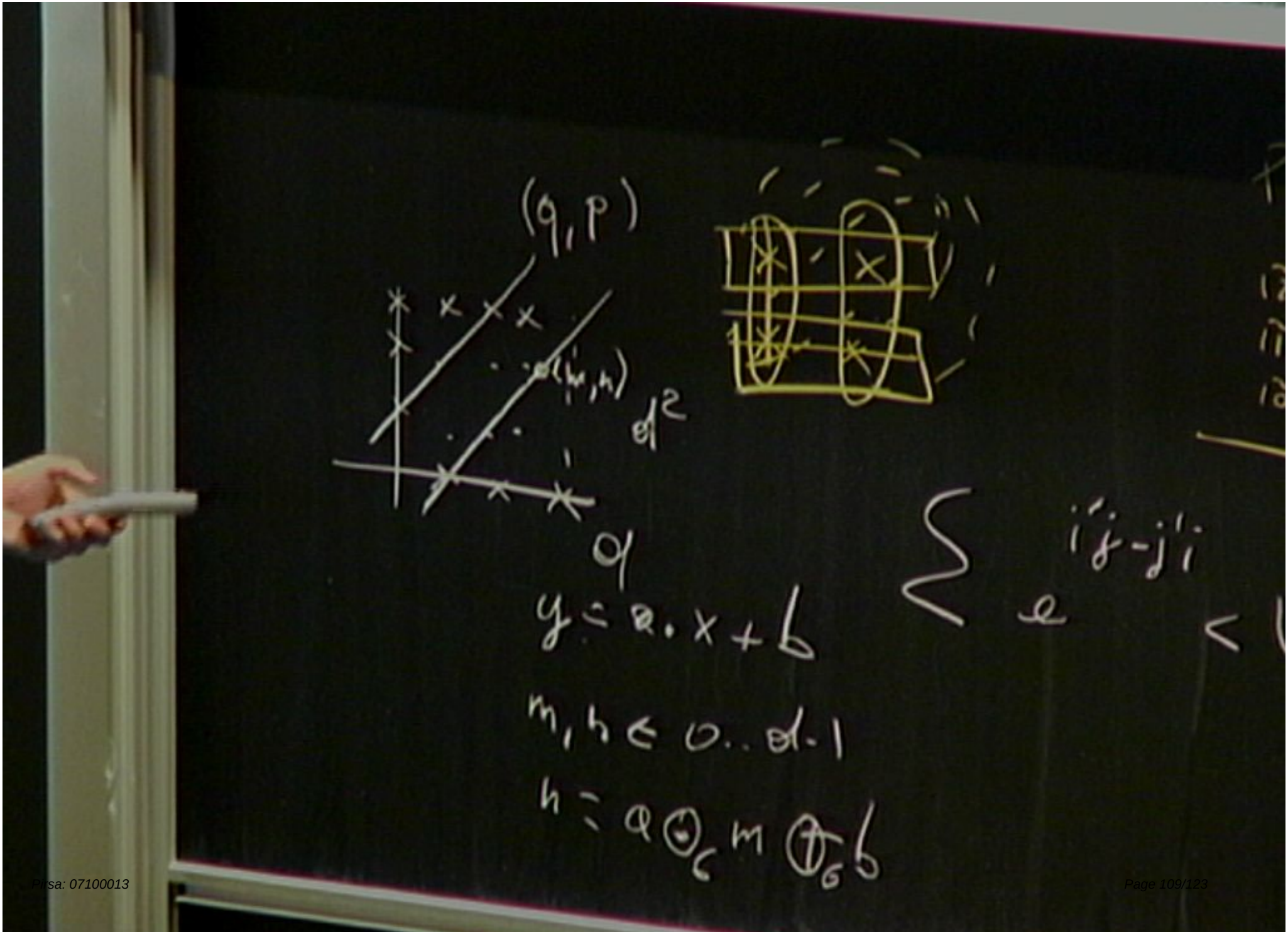

(q, p)
(m, n)
d²
q
y = a.x + b
m, n ∈ 0.. d-1
Σ
e
i'j-j'i

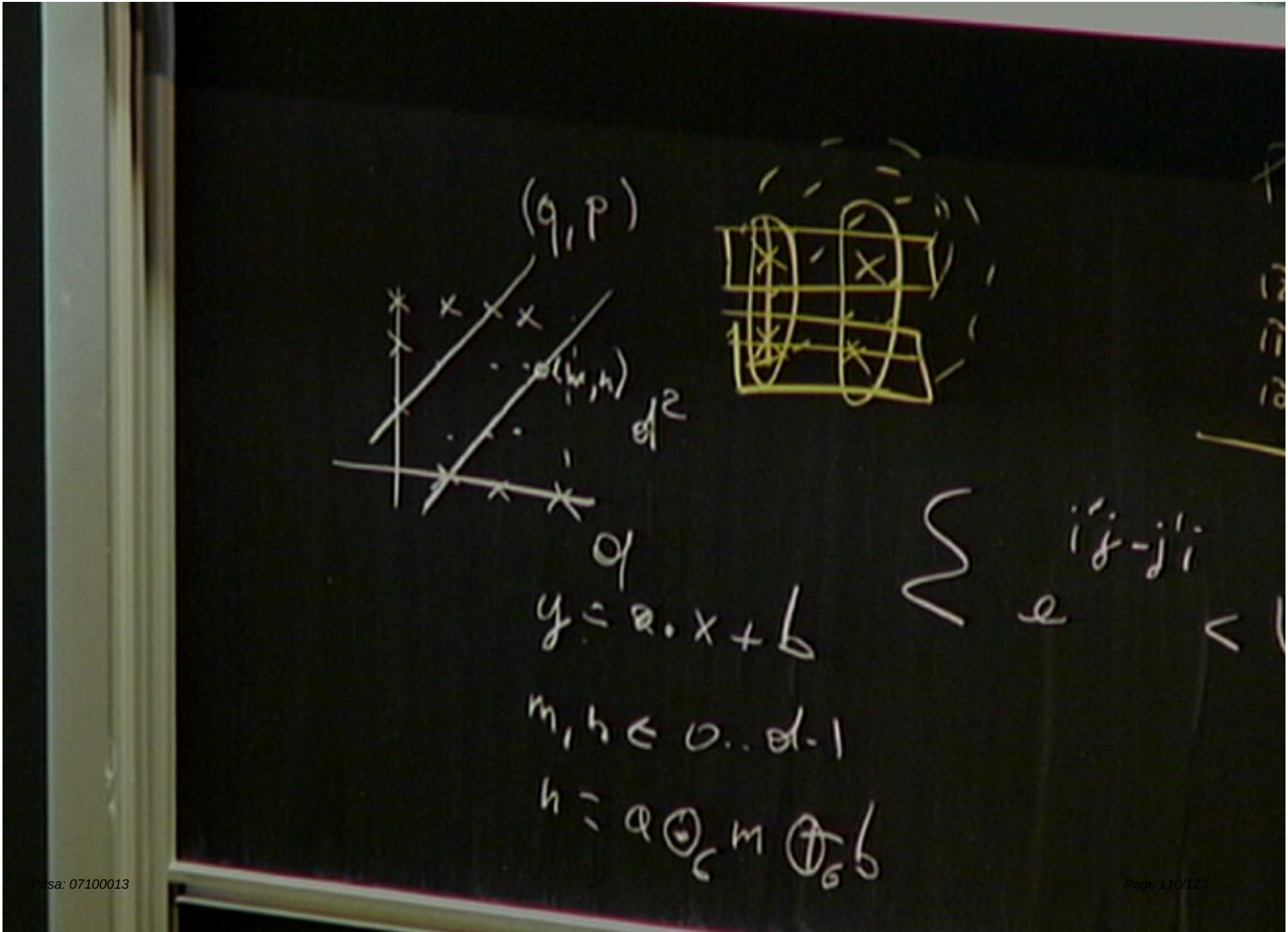

(q, p)
(m, n)
d²
q
y = a · x + b
m, n ∈ 0 .. d-1


(q, p)
d²
q
y = a · x + b
m, n ∈ 0 .. d-1
n = a ⊙ c


(q, p)
d²
q
y = a · x + b
m, n ∈ 0 .. d-1
n = q(m)
Σ
e
i i-j' i


(q, p)
d²
q
y = a · x + b
m, n ∈ 0 .. d-1


(q, p)
(m, n)
d²
q
y = a · x + b
m, n ∈ 0 .. d-1
h = a ⊙_c m ⊕_c b
Σ
e
i'j-j'i


(q, p)
(m, n)
d^2
q
y = a · x + b
m, n ∈ 0 .. d-1
h = a ⊙_c m ⊕_c b
Σ e^{i'j-j'i}

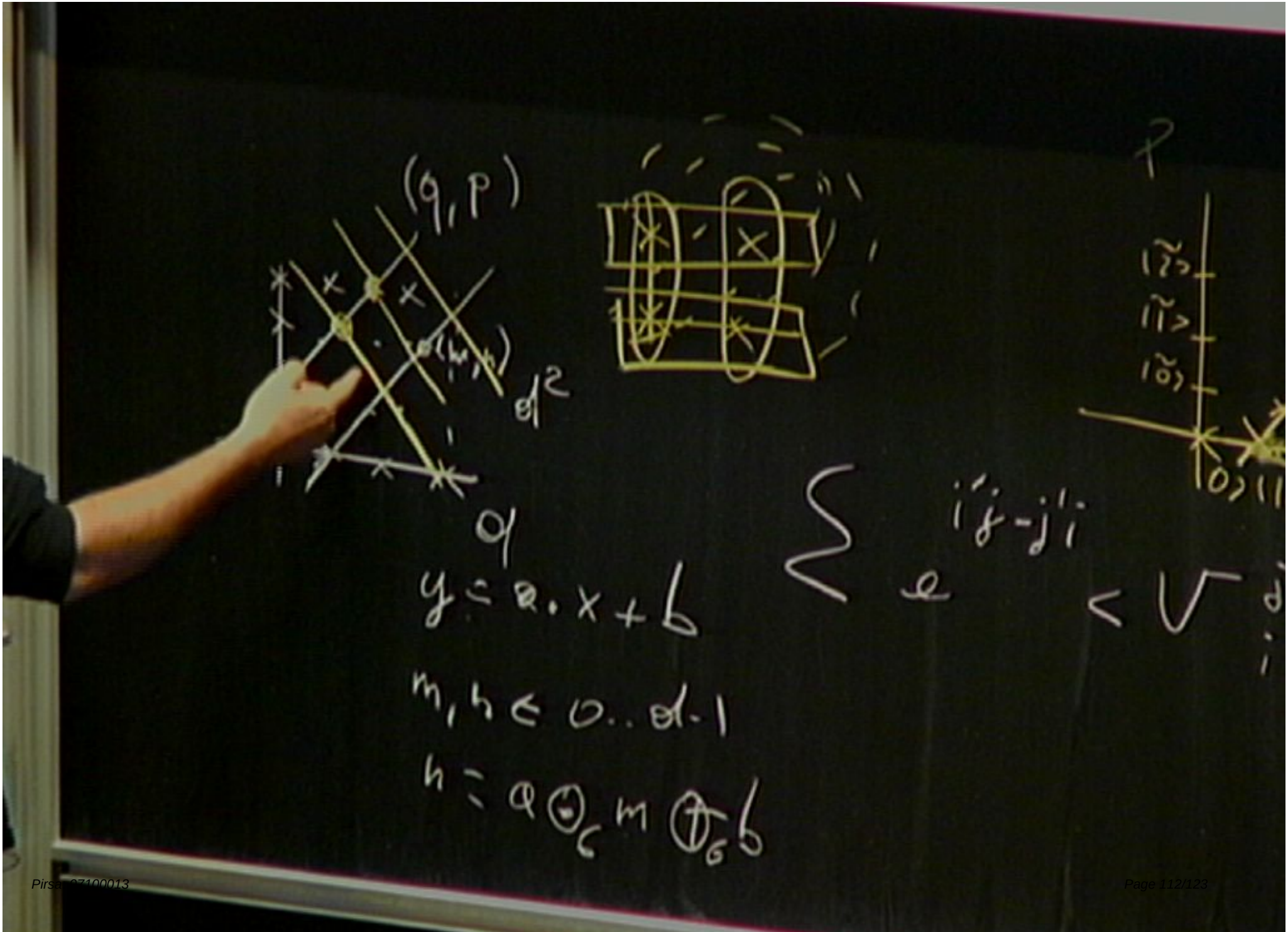
Geometrical correspondence.

-Two non-parallel straight lines intersect in only one point
because non-parallel directions correspond to different MUB's (states from different MUB's present an overlap $1/d$).

-Two distinct parallel lines do not intersect
because MUB's are orthogonal bases (different states of a same basis do not overlap).

There is thus a one-to-one correspondence between MUB's and an affine d times d plane.

-From this point of view, one has that to each straight line (there are $d^2 + d$ of them) corresponds a question, and when the state belongs to one of the MUB's, the questions are either deterministic (for d of them) or totally underteministic (for d^2 of them).


(q, p)
d²
q
y = a·x + b
m, n ∈ 0..d-1
n = a ⊙_c m ⊕_c b
P
|2⟩
|1⟩
|0⟩
|0⟩|1
Σ
e
|i-j|
<V

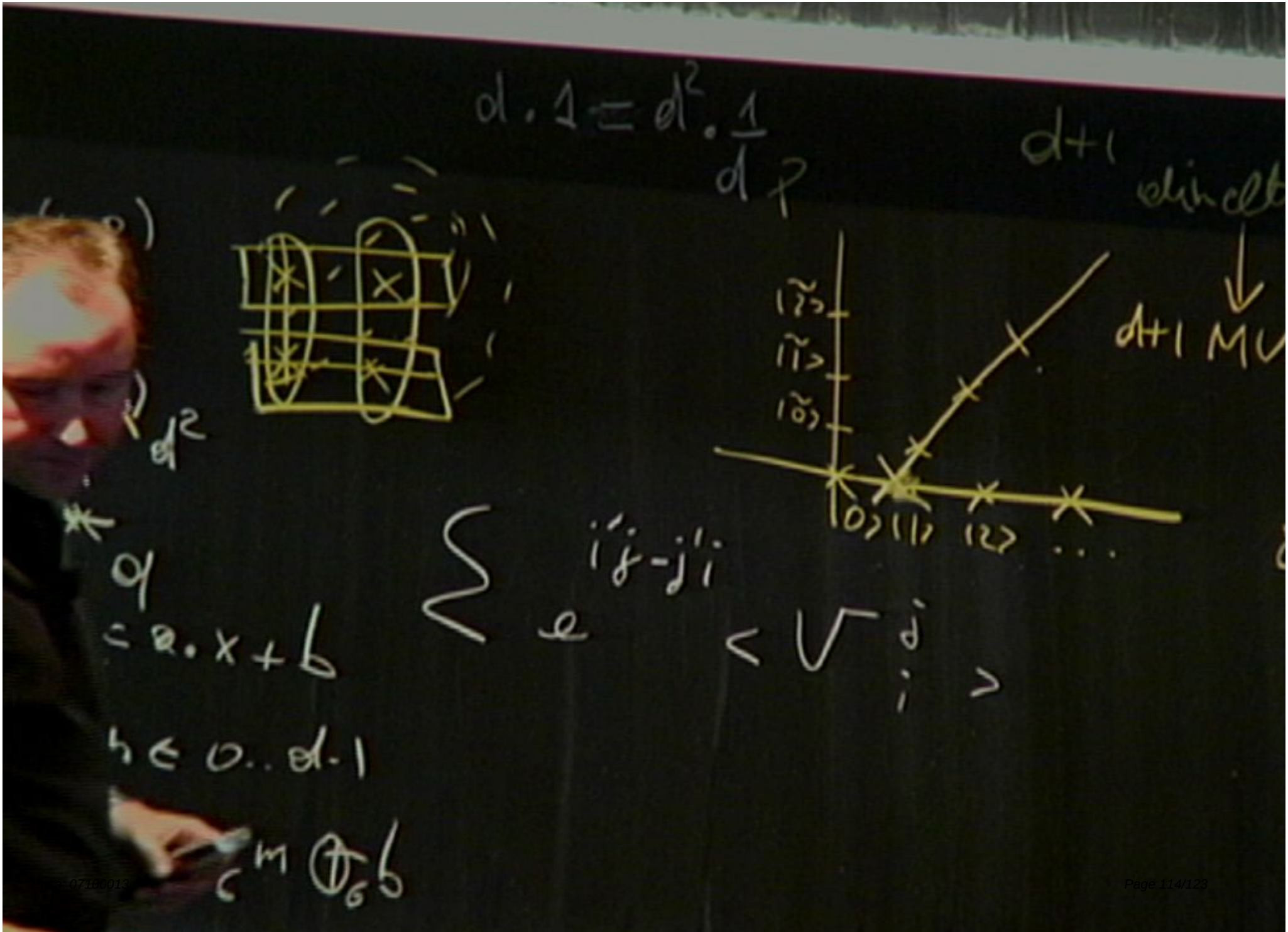
What do we learn from this about the epistemic interpretation?

-Roughly speaking, the epistemic interpretation (Robert W. Spekkens, "In defense of the epistemic view of quantum states: a toy theory", quant-ph/0401052) is **an attempt to develop an axiomatic framework in which the basic objects belong to a set of $d^2 + d$ questions, and of $d^2 + d$ states**.

-To each state would correspond d deterministic questions and d^2 undeterministic questions.

-In principle, the interpretation does not require to introduce the machinery of the Hilbert space.

-Nevertheless, it captures the main features of specific quantum properties such as MUB's, uncertainty relations, no cloning, teleportation and so on.


d . 1 = d² . 1/d p
d+1
d+1 M
|2̃⟩
|1̃⟩
|0̃⟩
|0⟩ |1⟩ |2⟩ ...
d²
q
= a . x + b
h ∈ 0 .. d-1
c^m mod_6 b
Σ e^{i'j-j'i} < V^j_i >
07180013
Page 114/123

What do we learn from this about the epistemic interpretation?

-Roughly speaking, the epistemic interpretation (Robert W. Spekkens, "In defense of the epistemic view of quantum states: a toy theory", quant-ph/0401052) is **an attempt to develop an axiomatic framework in which the basic objects belong to a set of $d^2 + d$ questions, and of $d^2 + d$ states**.

-To each state would correspond d deterministic questions and d^2 undeterministic questions.

-In principle, the interpretation does not require to introduce the machinery of the Hilbert space.

-Nevertheless, it captures the main features of specific quantum properties such as MUB's, uncertainty relations, no cloning, teleportation and so on.

We shall show that the epistemic interpretation cannot be pursued in all dimensions.
The reason therefore is that if the epistemic interpretation might be done, then we would be able
-to find sets of d^2 points that can be partitioned into $d+1$ sets of d parallel straight lines,
-with the property that non-parallel lines intersect in only one point, and that parallel distinct lines do not intersect.
Such a structure is called a finite affine plane, and it has been shown that such planes with d^2 points do not exist when $d = 6$ and $d = 10$.
It is conjectured that such planes exist only when d is a prime power.
This conjecture is fundamental in the study of finite geometries but explicit proofs exist only for $d = 6$ and $d = 10$. This is because the proofs are of combinatorial nature and the lenght of computation increases dramatically with the dimension.

Le problème des 36 officiers d'Euler

« Une question fort curieuse, qui a exercé pendant quelque temps la sagacité de bien du monde, m'a engagé à faire les recherches suivantes, qui semblent avoir une nouvelle carrière dans l'analyse, et en particulier dans la doctrine des combinaisons. Cette question rouloit sur une assemblée de 36 officiers de 6 différens grades et tirés de 6 régimens différens qu'il s'agissoit de ranger dans un carré, de manière que sur chaque ligne, tant horizontale que verticale, il se trouvât 6 officiers tant de différens caractères que de régimens différens. Or, après toutes les peines qu'on s'est données pour résoudre ce problème, on a été obligé de reconnoître qu'un tel arrangement est absolument impossible, quoiqu'on ne puisse pas en donner de démonstration rigoureuse.»

14 20 41 05 32 53
30 15 04 51 23 42
21 03 12 40 54 35
02 31 50 13 45 24
43 52 25 34 10 01
55 44 33 22

Ce problème est équivalent à trouver 2 carrés latins d'ordre 6 orthogonaux.

En 1900, un douanier algérien, Tarry, a prouvé par épuisement des cas qu'il n'existait pas de tels carrés latins.

Le problème des 36 officiers d'Euler

« Une question fort curieuse, qui a exercé pendant quelque temps la sagacité de bien du monde, m'a engagé à faire les recherches suivantes, qui semblent avoir une nouvelle carrière dans l'analyse, et en particulier dans la doctrine des combinaisons. Cette question rouloit sur une assemblée de 36 officiers de 6 différens grades et tirés de 6 régimens différens qu'il s'agissoit de ranger dans un carré, de manière que sur chaque ligne, tant horizontale que verticale, il se trouvât 6 officiers tant de différens caractères que de régimens différens. Or, après toutes les peines qu'on s'est données pour résoudre ce problème, on a été obligé de reconnoître qu'un tel arrangement est absolument impossible, quoiqu'on ne puisse pas en donner de démonstration rigoureuse.»

14 20 41 05 32 53
30 15 04 51 23 42
21 03 12 40 54 35
02 31 50 13 45 24
43 52 25 34 10 01
55 44 33 22

Ce problème est équivalent à trouver 2 carrés latins d'ordre 6 orthogonaux.

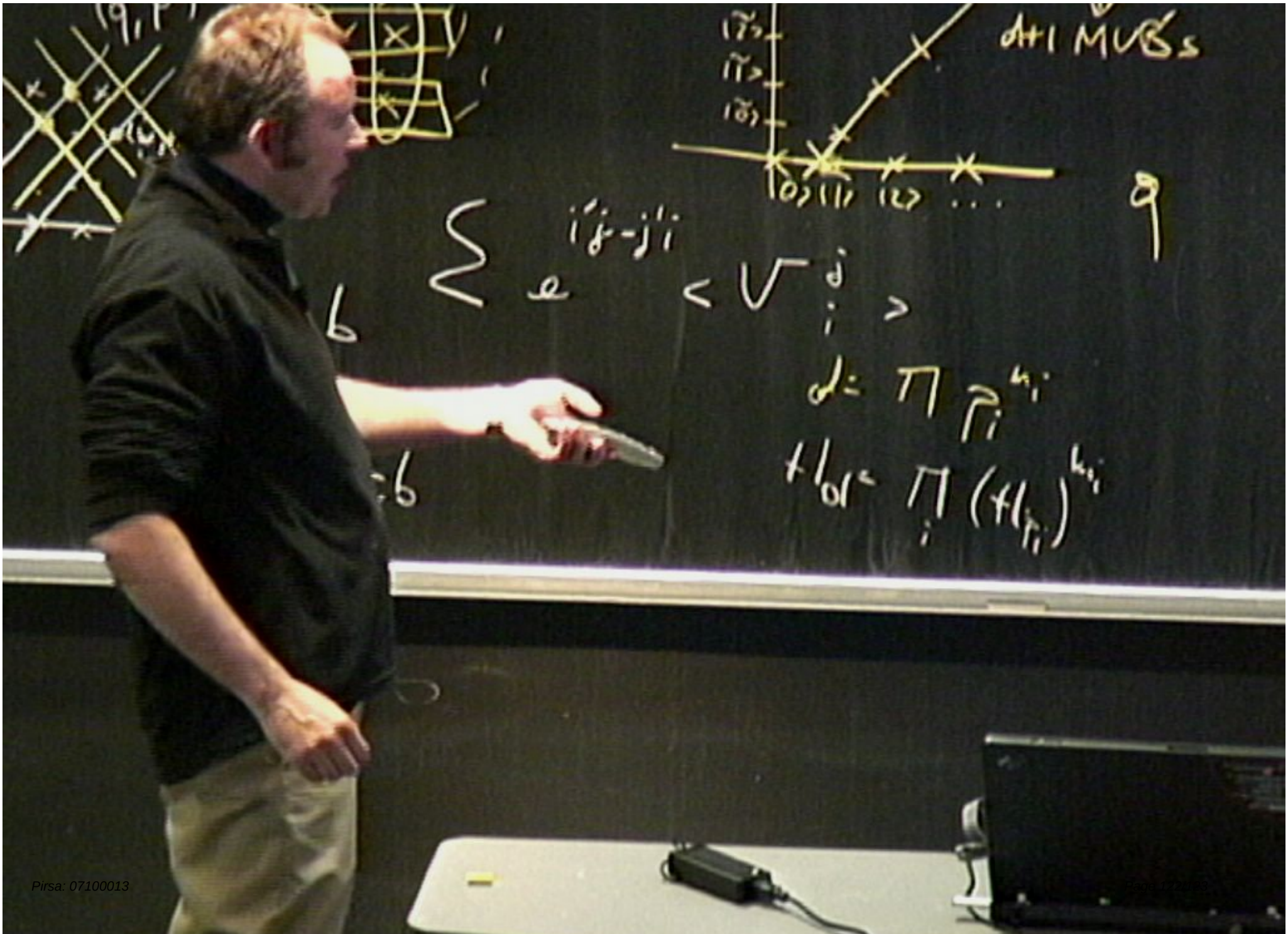
En 1900, un douanier algérien, Tarry, a prouvé par épuisement des cas qu'il n'existait pas de tels carrés latins.

This implies that no finite affine plane with 36 elements exist; otherwise 4 non parallel directions (associated to the 4 properties "regiment", "rank", "room", and "table") would provide a solution to the problem of the 36 officers.
As a consequence the epistemic approach cannot be followed in dimension 6. As d times d finite affine planes seemingly exist only for prime power dimensions, the epistemic approach seems to be confined to those dimensions.

TO CONCLUDE CERTAIN DIMENSIONS SEEM TO PLAY A SPECIAL ROLE IN QUANTUM INFORMATION,
PRIME DIMENSIONS SEEM TO BE "ATOMS OF DIMENSIONS",
AND THE FACTORISATION OF INTEGER DIMENSIONS INTO PRODUCTS OF PRIME POWERS COULD INDICATE A PHYSICAL FACTORIZATION OF FINITE DIMENSIONAL SYSTEMS INTO SUBSYSTEMS CONSTITUTED BY (EQUIVALENT) QuPits WITH P PRIME.

$$\langle V_i^{d} \rangle$$

$$d = \prod p_i^{m_i}$$



TO CONCLUDE CERTAIN DIMENSIONS SEEM TO PLAY A SPECIAL ROLE IN QUANTUM INFORMATION,
PRIME DIMENSIONS SEEM TO BE "ATOMS OF DIMENSIONS",
AND THE FACTORISATION OF INTEGER DIMENSIONS INTO PRODUCTS OF PRIME POWERS COULD INDICATE A PHYSICAL FACTORIZATION OF FINITE DIMENSIONAL SYSTEMS INTO SUBSYSTEMS CONSTITUTED BY (EQUIVALENT) QuPits WITH P PRIME.