

DE LA RECHERCHE À L'INDUSTRIE



INTRICATION EN RÉCITS

la science par ses homologues

www.cea.fr

Alexei Grinbaum (DRF/IRFU/LARSIM)

Quantum entanglement

Ryszard Horodecki

*Institute of Theoretical Physics
Poland*

Paweł Horodecki

*Faculty of Applied Physics and
Gdańsk, Poland*

Michał Horodecki

*Institute of Theoretical Physics
Poland*

Karol Horodecki

*Institute of Theoretical Physics
Poland
and Faculty of Mathematics, P
80-952 Gdańsk, Poland*



CONTENTS

I. Introduction	867
II. Entanglement as a Quantum Property of Compound Systems	873
III. Pioneering Effects Based on Entanglement	874
A. Quantum key distribution based on entanglement	874
B. Quantum dense coding	874
C. Quantum teleportation	875
D. Entanglement swapping	876
E. Beating classical communication complexity bounds with entanglement	876
IV. Correlation Manifestations of Entanglement: Bell Inequalities	877
A. Bell theorem: CHSH inequality	877
B. The optimal CHSH inequality for 2×2 systems	877
C. Violation of Bell inequalities by quantum states	878
1. Pure states	878
2. Mixed states	878

D. All $n \times 2 \times 2$ Bell inequalities for correlation functions	879
E. Logical versions of Bell's theorem	879
F. Violation of Bell inequalities: General remarks	879
V. Entropic Manifestations of Entanglement	880
A. Entropic inequalities: Classical versus quantum order	880
B. Entropic inequalities and negativity of information	880
C. Majorization relations	881
D. Other possible postulates	882
VI. Bipartite Entanglement	882
A. Definition and basic properties	882
B. Main separability criteria in the bipartite case	882
1. Positive partial transpose criterion	882
2. Separability via positive, but not completely positive, maps	883
3. Separability via entanglement witnesses	883
4. Estimating entanglement from incomplete data	885
5. Entanglement witnesses and Bell inequalities	886

6. Distinguishability map criteria: Reduction criterion and its extensions	886
7. Range criterion and its applications: PPT entanglement	887
8. Matrix realignment criterion and linear contraction criteria	888
9. Some important classes of quantum states	889
VII. Multiparticle Entanglement—Similarities and Differences	889
A. Notion of full (n -partite) separability	889
B. Further improvements of Entanglement Test: Nonlinear Separability Criteria	892
A. Uncertainty-rotation-based separability tests	892
B. Detecting entanglement with collective measurements	892
1. Physical implementations of entanglement criteria with collective measurements	892
2. Collective entanglement witnesses	893
C. Classical Algorithms Detecting Entanglement	893
X. Quantum Entanglement and Geometry	894
XI. The Paradigm of Local Operations and Classical Communication (LOCC)	896
A. Quantum channel: The main notion	896
B. LOCC operations	896
XII. Distillation and Bound Entanglement	897
A. One-way hashing distillation protocol	897
B. Two-way recurrence distillation protocol	898
C. Development of distillation protocols: Bipartite and multiparticle cases	898
D. All two-qubit entangled states are distillable	899
E. Reduction criterion and distillability	899
F. General one-way hashing	900
G. Bound entanglement: When distillability fails	900
H. The problem of NPT bound entanglement	900
I. Activation of bound entanglement	901
XIII. Manipulations of Entanglement and Irreversibility	902
A. LOCC manipulations on pure entangled states: Exact case	902
1. Entanglement catalysis	903
2. SLOCC classification	903
B. Asymptotic entanglement manipulations and irreversibility	903
1. Unit of bipartite entanglement	904
2. Bound entanglement and irreversibility	904
3. Asymptotic transition rates in multiparticle states	905
XIV. Entanglement and Quantum Communication	905
A. Capacity of quantum channel and entanglement	906
B. Formulas for capacities	907
C. Entanglement breaking and entanglement binding channels	907
D. Additivity questions	907
XV. Quantifying Entanglement	908
A. Distillable entanglement and entanglement cost	908
B. Entanglement measures: Axiomatic approach	909
1. Monotonicity axiom	909
2. Vanishing on separable states	909
3. Other possible postulates	910
C. Axiomatic measure: A survey	910
1. Entanglement measures based on distance	910
2. Coover root measures	911
a. Schmidt number	911
b. Concurrence	912
3. Other entanglement measures	912
a. Robustness measures	912
b. Negativity	912
c. Squashed entanglement	912
D. All measures for pure bipartite states	912
1. Entanglement measures and transition between states: Exact case	913
E. Entanglement measures and transition between states: Asymptotic case	913
1. E_F and E_C as extremal measures: Unique measure for pure bipartite states	913
2. Transition rates	914
F. Evaluation of measures	914
G. Entanglement imposes different orderings	915
H. Multiparticle entanglement measures	915
1. Multiparticle entanglement measures for pure states	915
I. How much can entanglement increase under communication of one qubit?	917
XVI. Monogamy of Entanglement	917
XVII. Entanglement in Continuous Variable Systems	917
A. Pure states	918
B. Mixed states	918
C. Gaussian entanglement	919
D. General separability criteria for continuous variables	920
E. Distillability and entanglement measures of Gaussian states	920
XVIII. Miscellaneous Facts About Entanglement	921
A. Entanglement under information loss: Locking entanglement	921
B. Entanglement and distillability states by LOCC	922
XIX. Entanglement and Secure Correlations	922
A. Quantum key distribution schemes and security proofs based on distillation of pure entanglement	922
1. Entanglement-distillation-based quantum key distribution protocols	923
2. Entanglement-based security proofs	924
3. Constraints for security from entanglement	925
4. Secure key beyond distillability of pure entanglement: Prolate	925
B. Drawing a private key from distillable and bound entangled states of the form ρ^{AB}	925
1. Devetak-Winter bound	925
2. Distillable key as an operational entanglement measure	926
3. Drawing a secure key from bound entanglement	926
C. Private states: New insight into entanglement theory of mixed states	927
D. Quantum key distribution schemes and security proofs based on distillation of private states: Private key beyond pure entanglement	927
E. Entanglement in other cryptographic scenarios	927
F. Interrelations between entanglement and classical key agreement	928
1. Classical key agreement: Analogy to	928

distillable entanglement scenario 928

2. Is there a bound information? 929

XX. Entanglement and Quantum Computing 929

 A. Entanglement in quantum algorithms 929

 B. Entanglement in quantum architecture 930

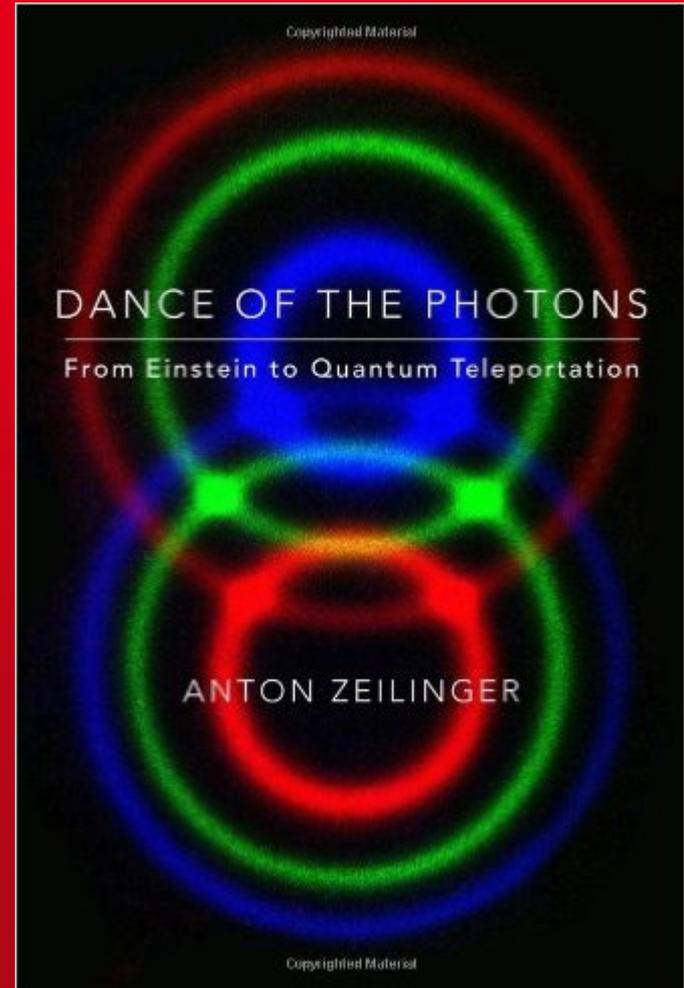
 C. Byzantine agreement: Useful entanglement for quantum and classical distributed computation 931

Acknowledgments 931

References 931

Quantum billiard balls are much stranger than classical ones. They will also move away from each other after the collision, but with these interesting and very strange differences. Neither of the two balls has a well-defined speed, nor does it move in a specific direction. Actually, neither of the balls has a speed or direction after the collision. They just move apart from each other.

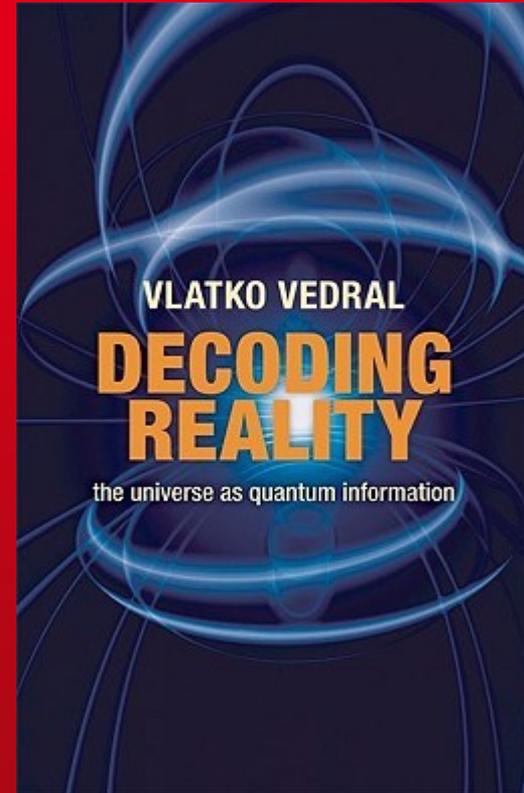
The crucial point is this: as soon as we observe one of the quantum billiard balls, the ball instantly assumes a certain speed and moves along a certain direction away from the collision. At that very moment—but not before—the other ball assumes the corresponding speed and direction. And this happens no matter how far apart the two balls are. So, quantum billiard balls are entangled. Einstein did not like this strange feature, and he called it “spooky action at a distance”.



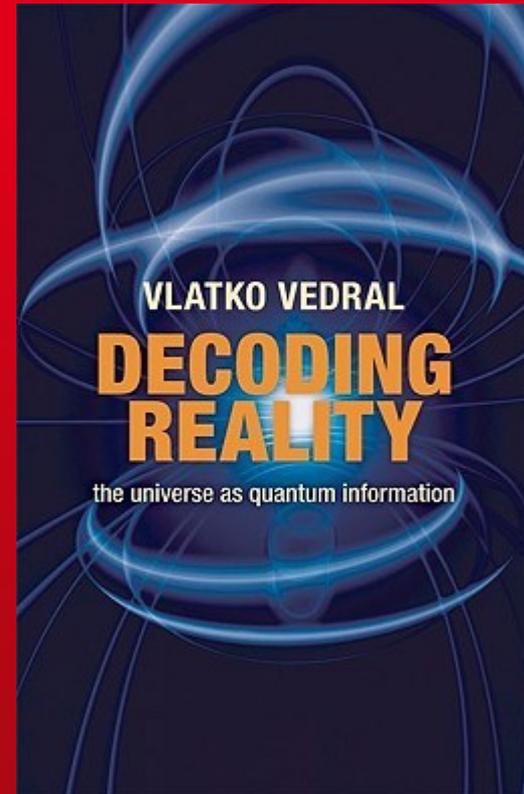
In classical physics, spins at different times can be correlated in the horizontal or vertical direction, so that, if the first measurement of spin yields 'horizontal clockwise,' so does the second measurement, in which case the mutual information between them is 100%. Real electrons behave quantum mechanically and their spin measurements could be correlated in the vertical direction at the time as the horizontal direction (and all other directions!).

This is because electrons can spin simultaneously in the clockwise and counterclockwise directions, something that no spinning top can do. In this case we can say that they may share up to 200% information.

This super-correlation is known as quantum entanglement, or 'spooky action at a distance' as Einstein referred to it.



It seems very counterintuitive. Two spinning electrons are created in such a way that there is absolutely no uncertainty about their overall state, but, if we look at each of them individually, it looks like a complete mess. In other words, they need each other to fully describe their state. This does not happen classically: if one of the systems is in a mess, then adding another system cannot decrease the amount of mess. Some might say the two electrons are like 'identical twins'—there is some mutual information 'beyond the norm'.



Springer Theses
Recognizing Outstanding Ph.D. Research

Jean-Daniel Bancal

On the Device-Independent Approach to Quantum Physics

Advances in Quantum
Nonlocality and Multipartite
Entanglement Detection

PAGE

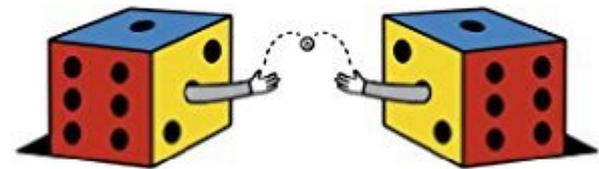
 Springer

6

NICOLAS GISIN

L'IMPENSABLE HASARD

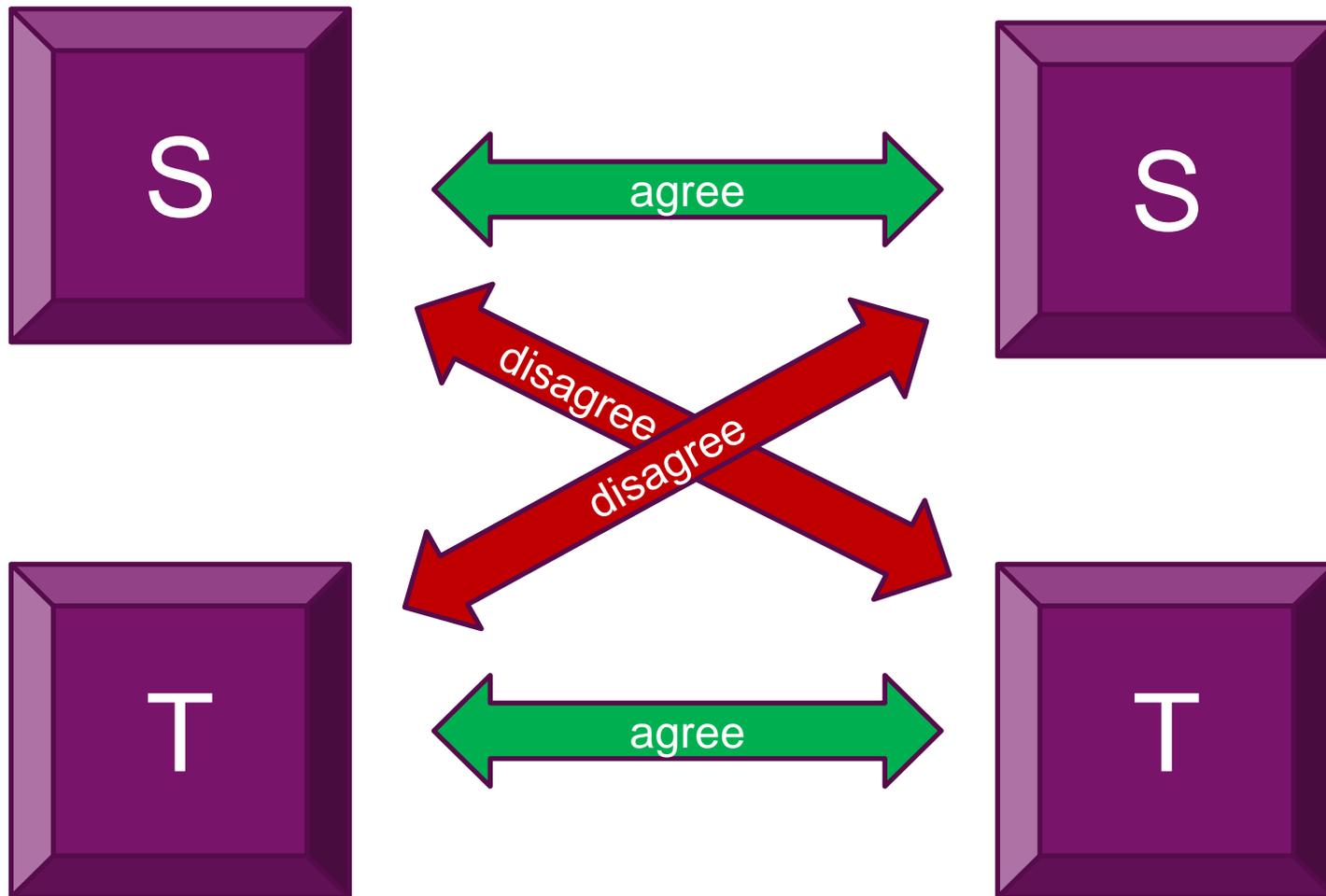
NON-LOCALITÉ, TÉLÉPORTATION
ET AUTRES MERVEILLES QUANTIQUES

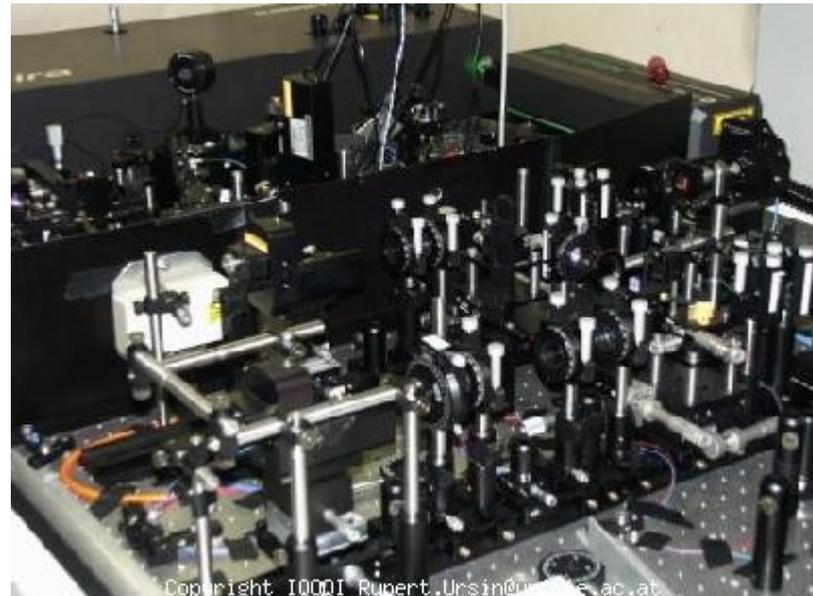
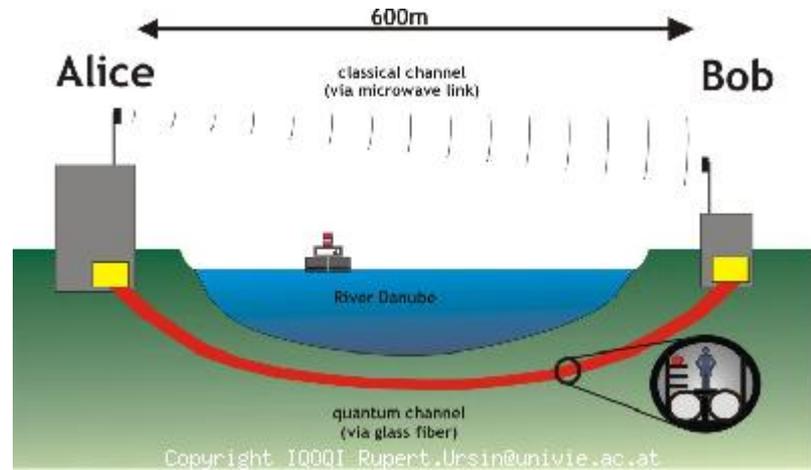
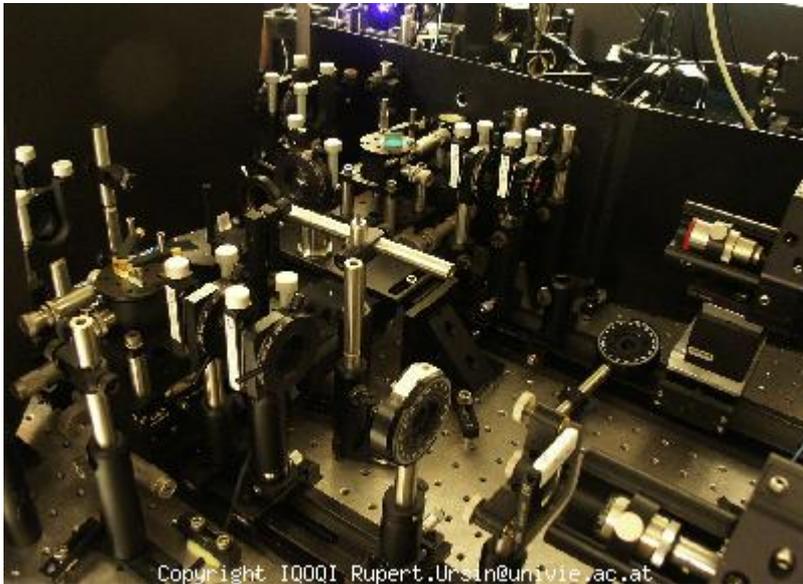


préface de
Alain Aspect

Odile
Jacob
sciences

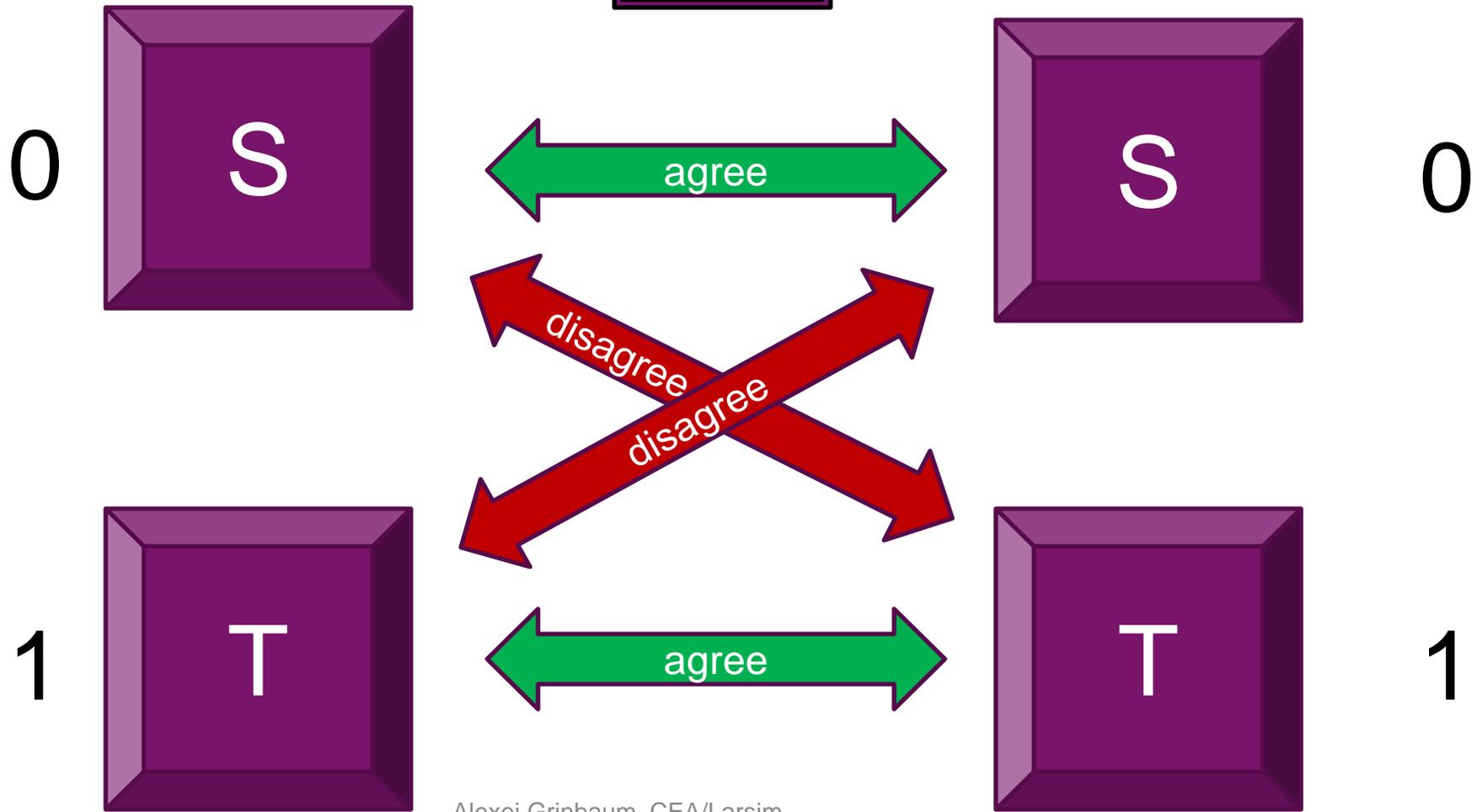
NON-LOCAL GAME



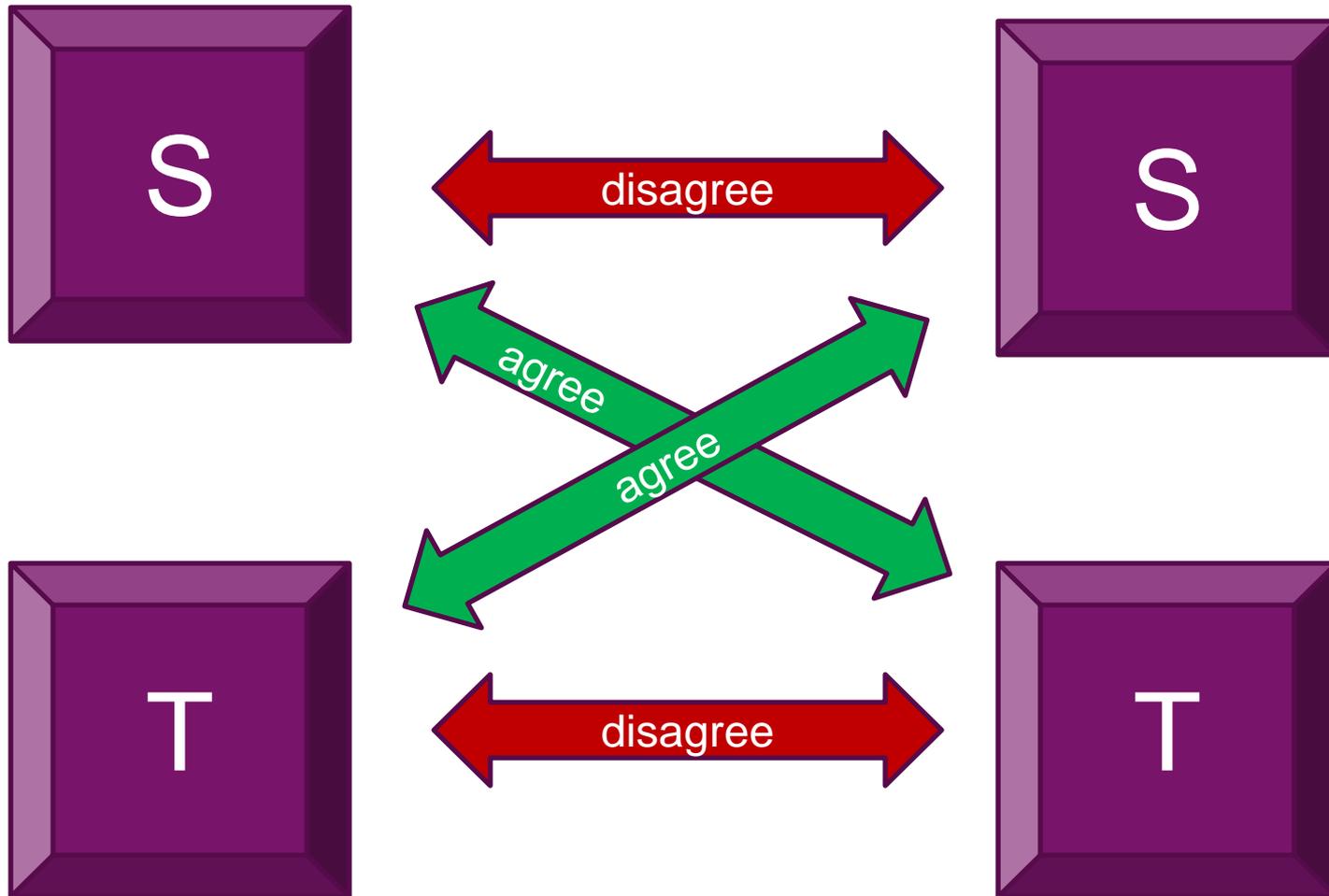


NON-LOCAL GAME

100% win

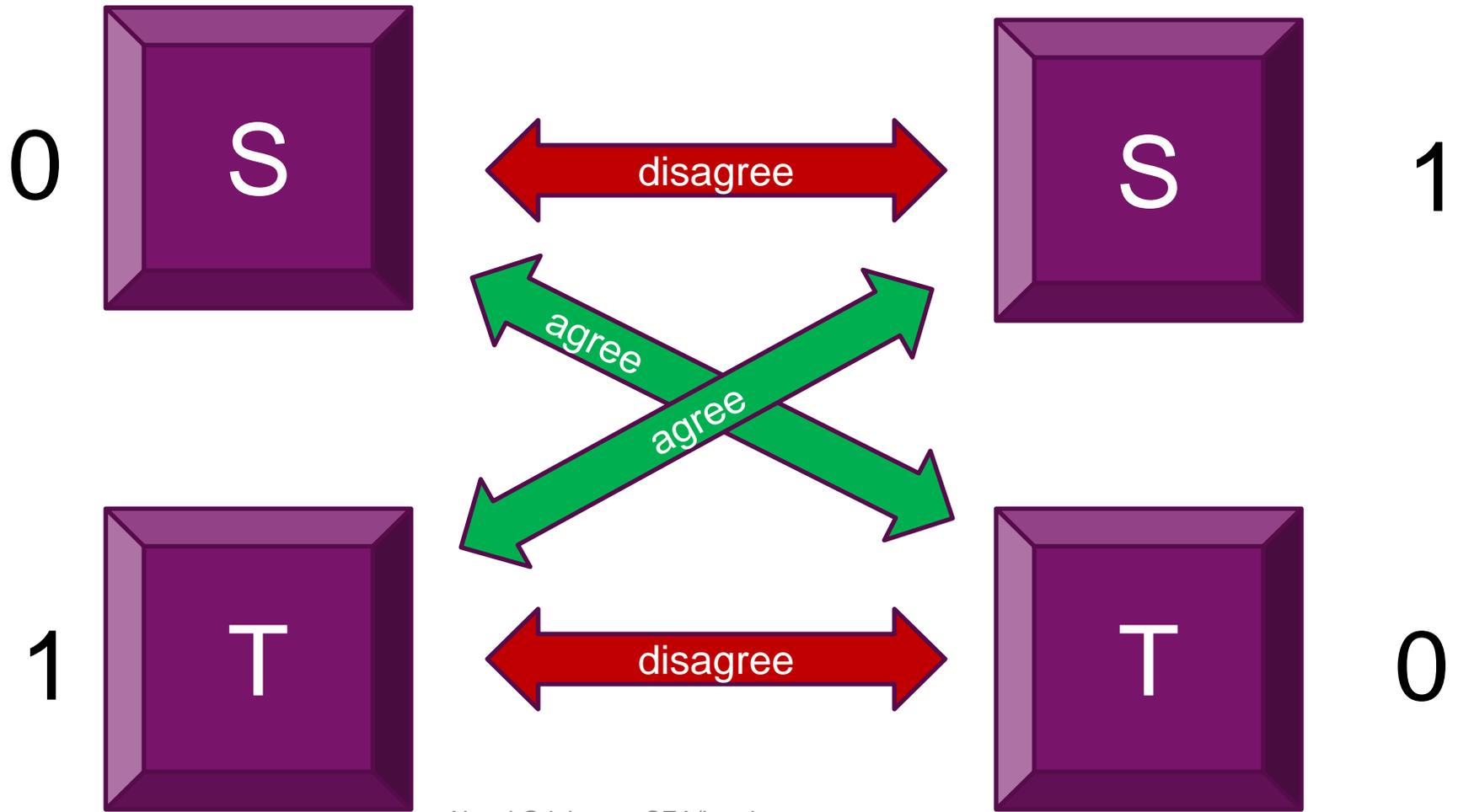


NON-LOCAL GAME

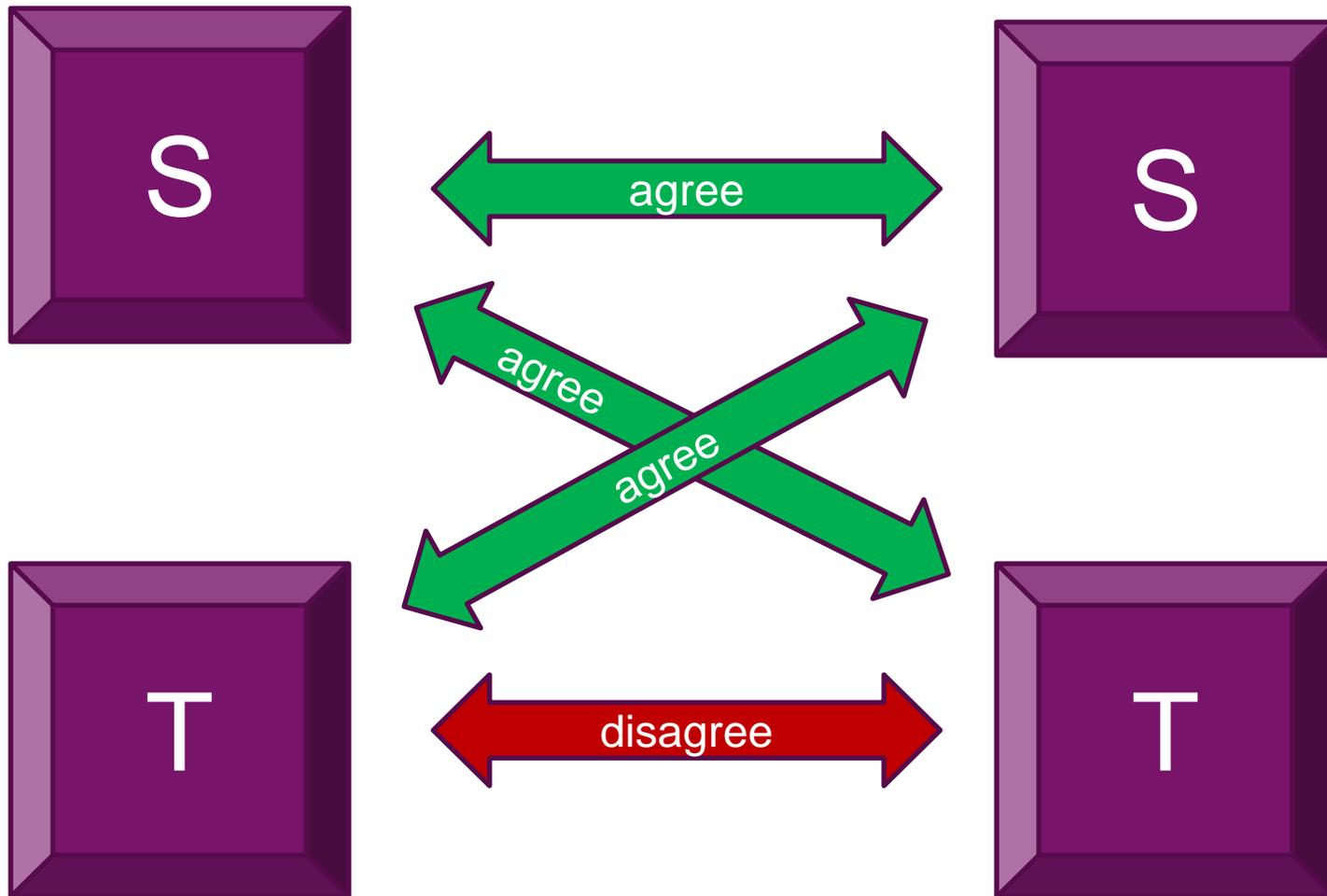


NON-LOCAL GAME

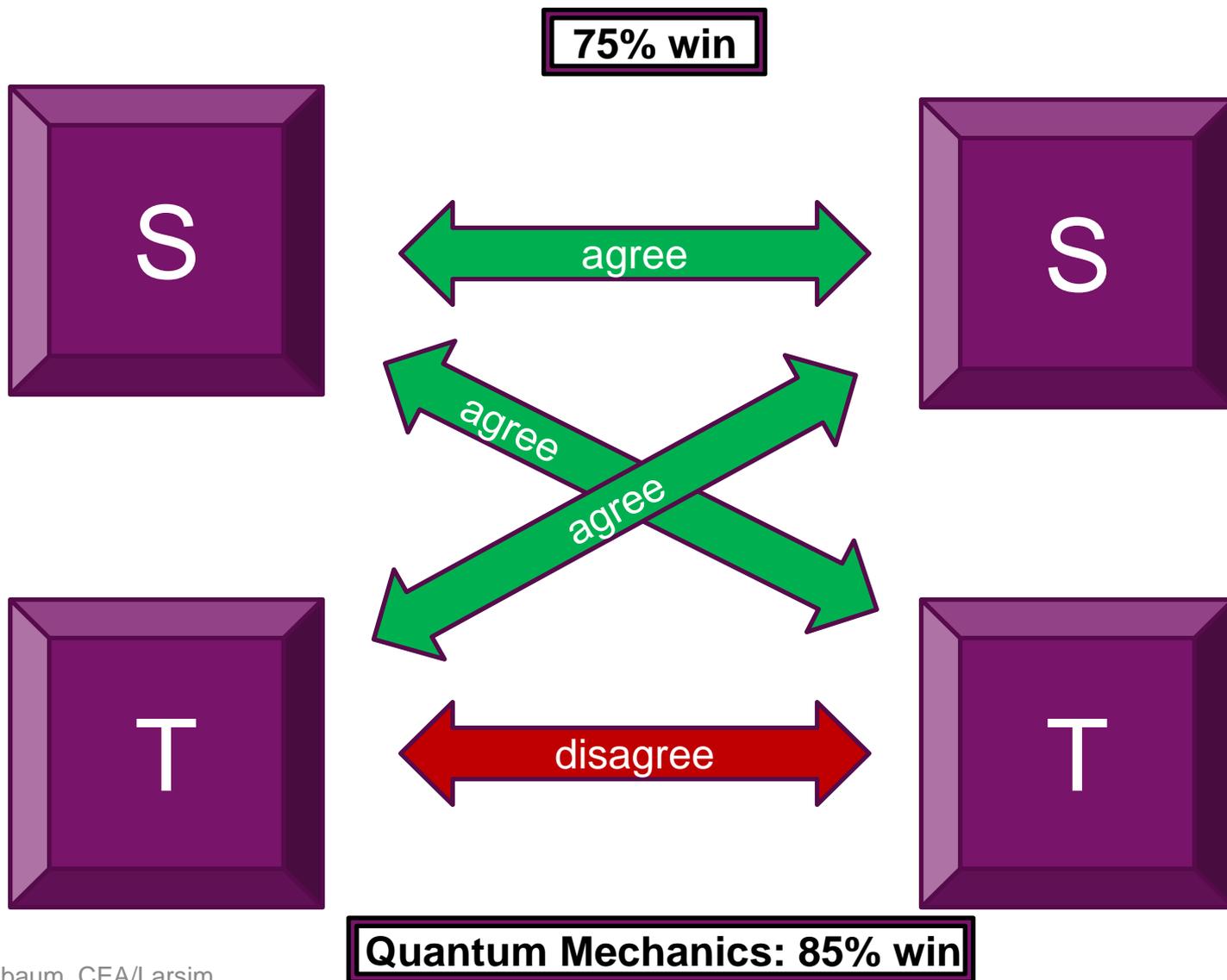
100% win



NON-LOCAL GAME



NON-LOCAL GAME



CE QUE TRANSMET LA VULGARISATION

- Vérité
- Beauté
- Magie du résultat



à la recherche d'une méthode

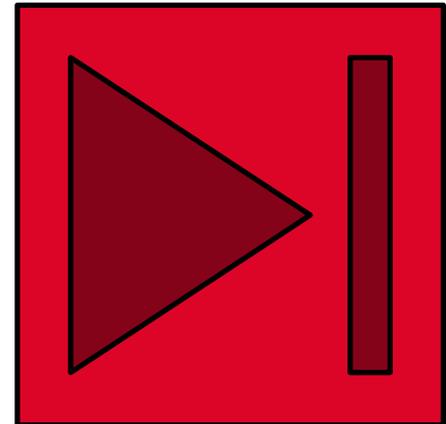
LA VOIE DE L'HOMOLOGIE



II SIÈCLE

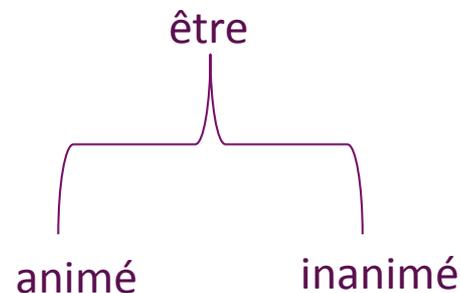
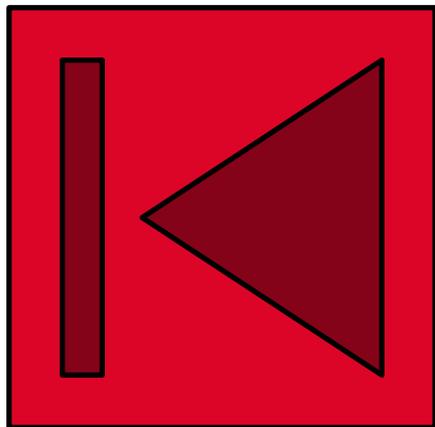
DIEU DANS LA DOCTRINE HERMÉTIQUE

1. Dieu est soustrait à la connaissance sensible.
2. Dieu est soustrait à la connaissance rationnelle et par dénomination (parce que au-dessus de tout nom).
3. Dieu n'est pas connaissable positivement. On ne peut dire que ce qu'il n'est pas.
4. Dieu est susceptible d'une connaissance suprationnelle ou mystique.



CELSE SUR LA CONNAISSANCE DE DIEU

Platon est un docteur plus efficace en matière de théologie, lui qui nous dit dans le *Timée* : « Découvrir le Créateur et Père de cet univers est chose difficile ; quand on l'a découvert, l'expliquer à tous est impossible ». Voyez donc comment les hommes inspirés de Dieu cherchent la Voie de Vérité.



Mais puisqu'enfin les sages ont trouvé une méthode pour nous faire acquérir quelque notion de l'Innommable et Premier, qui rend Dieu manifeste :

- soit par la synthèse qui embrasse et domine les autres notions,
- soit par séparation (« analyse ») d'avec ces autres notions,
- soit par analogie,

je veux vous enseigner ce qui par ailleurs est ineffable : mais je serais bien étonné si vous pouviez me suivre, vous qui êtes entièrement prisonniers de la chair et dont le regard n'a rien de pur.

“My way of thinking is now this: properly considered, one cannot get at the Talmudist if one does not make use of a supplementary principle: the ‘separation principle’. That is to say: ‘the second box, along with everything having to do with its contents, is independent of what happens with regard to the first box (separated partial systems).’ If one adheres to the separation principle, then one thereby excludes the second (‘Schrödinger’) point of view, and only the Born point of view remains, according to which the above state description is an incomplete description of reality, or of the real states.”
(Einstein to Schrödinger, 19 June 1935)

“This happens no matter how far apart the two balls are.” (Zeilinger)

- Dieu est incirconscrit (Apulée, II siècle).
- Dieu est sans parties (Albinus, II siècle)
- La vraie connaissance de Dieu n’est pas telle qu’elle le circonscrive comme une essence déterminée (Damascius, VI siècle).

HOMOLOGIE AVEC LE MYTHE : LES DANGERS

Platon « Le mythe est un récit faux où il se trouve du vrai »

Plutarque « L'élément mythique de ce récit touche à une vérité physique »

Brisson « Le récit d'un mythe est assimilé à un voyage qui constitue un danger dont on est sauvé, lorsqu'on est arrivé sain et sauf à bon port »

HOMOLOGIE AVEC LE MYTHE : LES AVANTAGES

The Dialectics of Myth

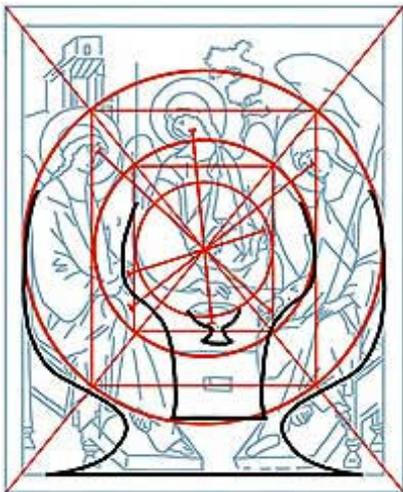
Aleksei Fyodorovich Losev

translated from the Russian by
Vladimir Marchenkov



Mythical consciousness is totally immediate and naïve, and can be understood by everyone; by contrast, scientific consciousness necessarily has a deductive and logical character: it is mediated, difficult to absorb, and requires long training in the skills of abstract thinking. Myth is always synthetic and vital, and always consists of live persons whose fate is depicted with emotion and palpable intimacy. Science, on the other hand, always turns life into a formula, giving abstract schemata and formulae instead of living persons; and its realism and objectivism consist not in a colourful description of life, but in the correct correspondence of abstract law and formula to the empirical flux of phenomena – quite apart from the picturesque and emotional quality of myth.

LA PÉRICHORÈSE ET LES TYPES DE MÉLANGES



DE LA RECHERCHE À L'INDUSTRIE

cea



UNE HISTOIRE DE LA COMPOSITION

www.cea.fr

Alexei Grinbaum, CEA/Larsim



Héraclès est né grâce à une ruse. Zeus couche avec Alcmène, mère d'Héraclès, en prenant l'apparence d'Amphitryon, son mari.

Plaute raconte qu'il a même « si bien pris la figure d'Amphitryon, que tous les esclaves qui l'aperçoivent pensent voir leur maître : tant il est habile à changer de peau, quand il lui plaît ! »

Amphitryon 121-123

Le récit littéraire est le seul moyen qui nous permet de distinguer le Zeus déguisé en Amphitryon d'Amphitryon lui-même. Alcmène, qui n'a pas d'accès à ce moyen, laisse Zeus entrer dans sa couche. Elle ne sait pas que c'est Zeus ; pour elle, son concubin *est* Amphitryon. Tout se passe comme s'il existait deux Amphitryons : le « vrai » et son double.

Supposons qu'un premier système quantique, « Amphitryon », soit dans l'état que nous écrivons en notation de Dirac comme $|0\rangle_A$. Indice « A » signifie « Amphitryon ». Le deuxième système, « Zeus », peut initialement assumer n'importe quel état que nous notons $|\psi\rangle_Z$. Indice « Z » signifie les états respectifs de Zeus.

A la fin de la métamorphose au cours de laquelle Zeus prend les apparences d'Amphitryon, son état doit être le même que celui d'Amphitryon :

$$|0\rangle_A \otimes |\psi\rangle_Z \xrightarrow{\text{devient}} |0\rangle_A \otimes |0\rangle_Z.$$

Qui plus est, la forme de cette transformation reste la même pour tous les états possibles d'Amphitryon. Si celui-ci est initialement dans l'état $|1\rangle_A$, la même métamorphose doit avoir lieu :

$$|1\rangle_A \otimes |\psi\rangle_Z \xrightarrow{\text{devient}} |1\rangle_A \otimes |1\rangle_Z.$$

Or la mécanique quantique permet de considérer également un état initial arbitraire d'Amphitryon, que nous pouvons représenter en tant que superposition des états $|0\rangle_A$ et $|1\rangle_A$:

$$a |0\rangle_A + b |1\rangle_A.$$

Les coefficients a et b sont deux nombres complexes. Puisque dans l'espace de Hilbert la somme des probabilités doit être égale à 1, ils obéissent à la condition :

$$a^2 + b^2 = 1.$$

Cet état générique, inconnu, de mixtion, quel qu'il soit, est lui aussi susceptible d'être cloné par Zeus à l'aide de la même transformation de dédoublement :

$$(a |0\rangle_A + b |1\rangle_A) \otimes |\psi\rangle_Z \xrightarrow{\text{devient}} (a |0\rangle_A + b |1\rangle_A) \otimes (a |0\rangle_Z + b |1\rangle_Z).$$

$$(a |0\rangle_A + b |1\rangle_A) \otimes |\psi\rangle_Z \xrightarrow{\text{devient}} (a |0\rangle_A + b |1\rangle_A) \otimes (a |0\rangle_Z + b |1\rangle_Z).$$

Ouvrons les parenthèses du côté gauche de la flèche. On y trouve deux termes :

Terme dans la somme à gauche	Coefficient devant ce terme
$ 0\rangle_A \otimes \psi\rangle_Z$	a
$ 1\rangle_A \otimes \psi\rangle_Z$	b

Chacun de ces termes est un état quantique d'Amphitryon, qui après clonage donne deux exemplaires de soi-même.

Du côté droit de la flèche, on trouve une somme, non pas de deux, mais de quatre termes :

Terme dans la somme à droite	Coefficient devant ce terme
$ 0\rangle_A \otimes 0\rangle_Z$	a^2
$ 1\rangle_A \otimes 1\rangle_Z$	b^2
$ 0\rangle_A \otimes 1\rangle_Z$	ab
$ 1\rangle_A \otimes 0\rangle_Z$	ba



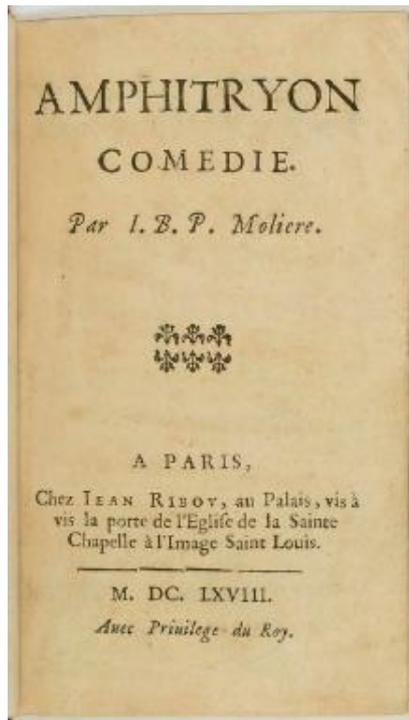
TÉLÉPORTATION

Hélène, à la fin du troisième chant de l'Iliade, se trouve dans une situation intéressante. Son ravisseur troyen, Pâris, est en train de perdre un combat singulier contre Ménélas, époux achéen d'Hélène. Sur le point d'être cloué par l'épée de Ménélas, Pâris est « facilement » sauvé par Aphrodite, qui l'entoure d'un nuage épais et le transporte dans la chambre nuptiale de sa maison.

Immédiatement après, Aphrodite, déguisée en vieille femme, apparaît devant Hélène, à qui elle commande de rejoindre aussitôt la pièce où repose Pâris (qu'elle appelle par son autre nom d'Alexandros). Voici ce que dit la déesse à propos de cet homme tout juste blessé, dont le « cou délicat » fut presque étouffé par les crins de son casque :

« Alexandros t'invite à revenir. Il est couché, plein de beauté et richement vêtu, sur son lit habilement travaillé. Tu ne dirais point qu'il vient de lutter contre un homme, mais tu croirais qu'il va aux danses, ou qu'il repose au retour des danses. »

Quelle scène invraisemblable ! Non seulement Aphrodite transporte-t-elle Pâris très rapidement d'un endroit à un autre, l'ayant recouvert d'un épais nuage ; mais elle remplace aussitôt son corps fatigué, blessé, par un corps plein de beauté et dominé entièrement par le désir, à tel point qu'Alexandros dira à Hélène quelques instants plus tard que « jamais le désir ne m'a brûlé ainsi ». Est-ce en fait le même homme ?



Messieurs, ce mot termine
Toute l'irrésolution:
Le véritable Amphitryon,
Est l'Amphitryon, où l'on dîne.

