Reinhard F. Werner
Inst. Mathematical Physics
TU Braunschweig

# Quantum Information Theory and Quantum Algorithms: overview and current status

Information Society Technologies

The Making of a Quantum Computer
- Quantum Information in the
6th Framework Programme
March 11, 2003

# Outline

- General remarks+Road Map
- Capacity and error correction
- Entanglement qualitative & quantitative
- Algorithms

**Disclaimer**

I will **not** give proper credit to anyone (including myself)

QUIPC-Cluster tags would be all over the place
EQUIP, QAIP, Q-ACTA + others

# Quantum Information Theory

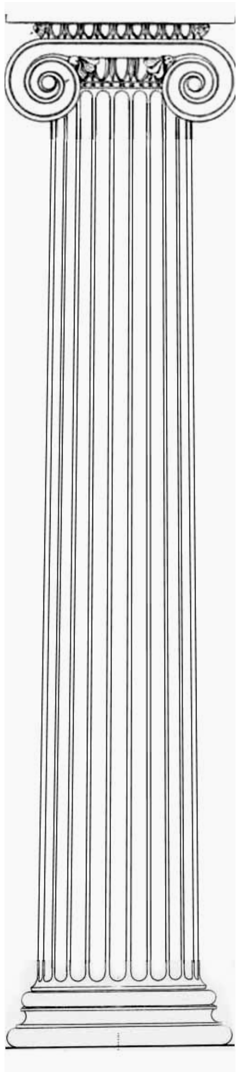
is by definition **abstract**

i.e., “a qubit is a qubit“ (Shannon: bit=bit )

This complements system-specific theory

But it is from here that the guiding
new ideas of the field come …

# The Classics of Quantum Information

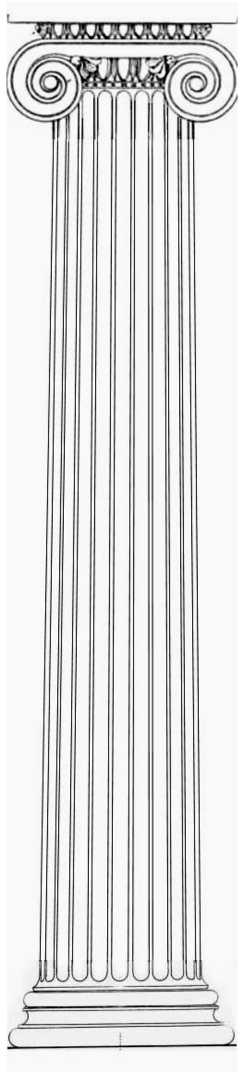


Algorithms of Shor & Grover

Entanglement distillation
Error correcting codes

Cryptography, Teleportation

Information Physics
Quantitative Turn



From ≈1997 the development was less dramatic.

Breakthroughs were much harder to get.

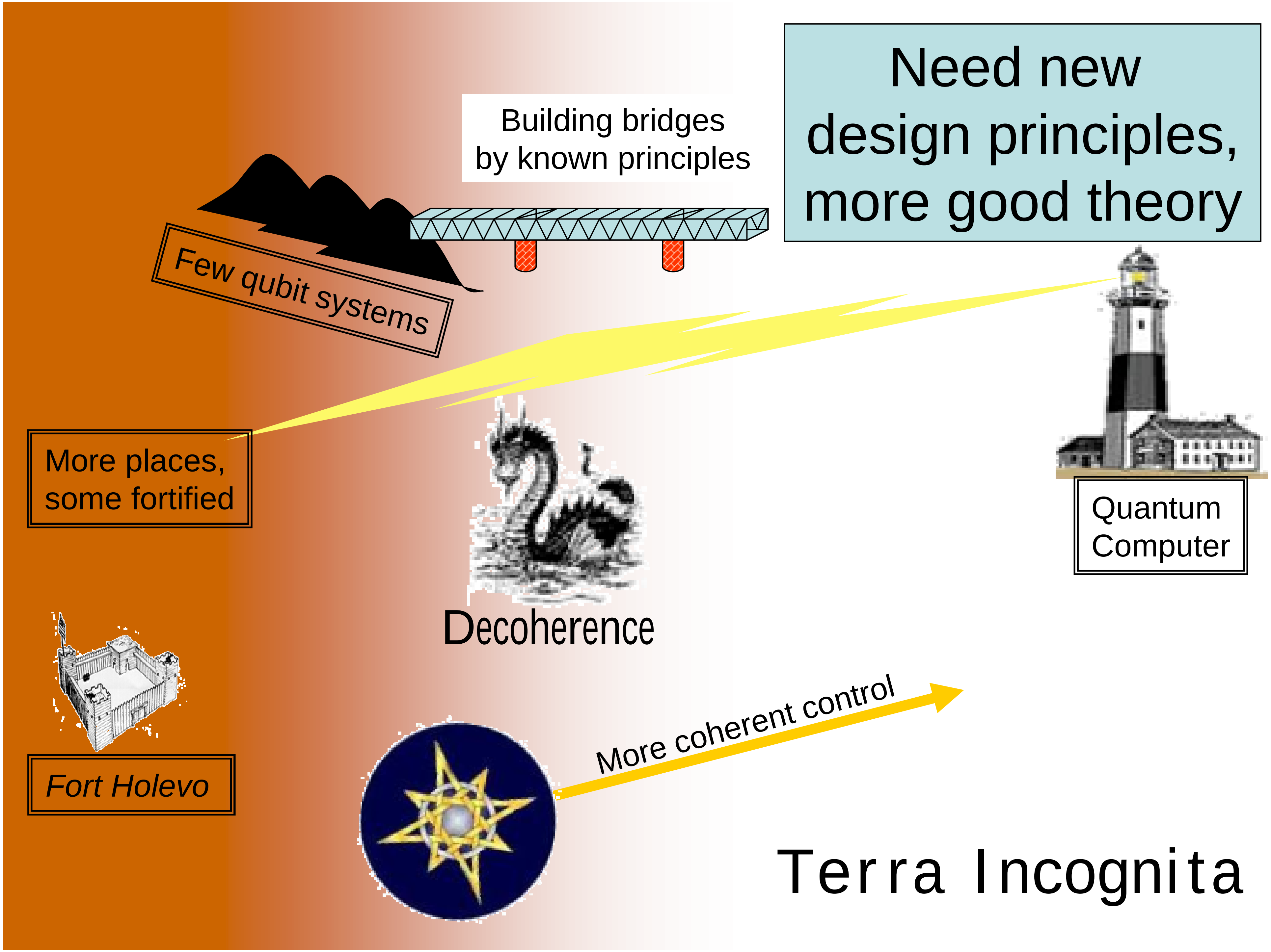
# Why ?

- Rapid growth of dimension

  Numerical simulations get stuck quickly
  to be expected!!! (without Q-Computer)

- Lack of analytic concepts to tame this growth

- Shor algorithm is really quite subtle
  no single reason why it works


Need new
design principles,
more good theory
Building bridges
by known principles
Few qubit systems
More places,
some fortified
Quantum
Computer
Decoherence
Fort Holevo
More coherent control
Terra Incognita

# Quantum

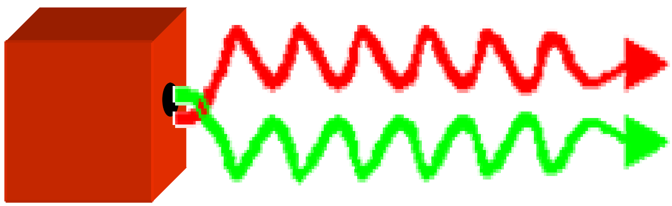
# Correlation & Information

- a unified quantitative view -

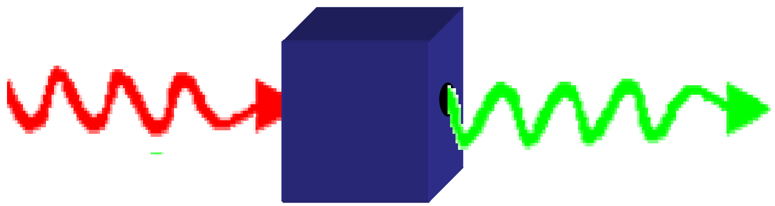
Entanglement | Capacity

a property of

(bipartite) states



channels

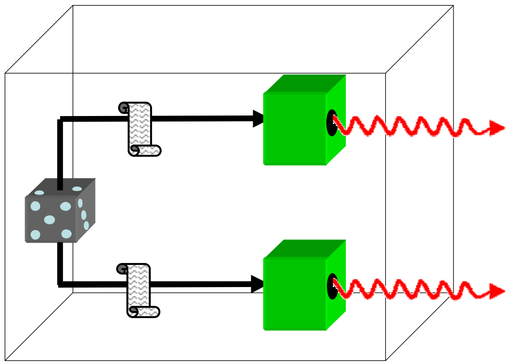


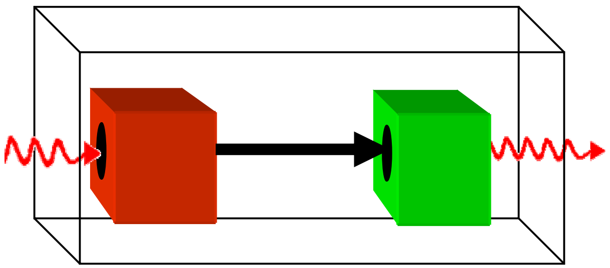
Entanglement Capacity

cannot

be generated by a classical random generator for “hidden variables“.

be transmitted via a classical chanel



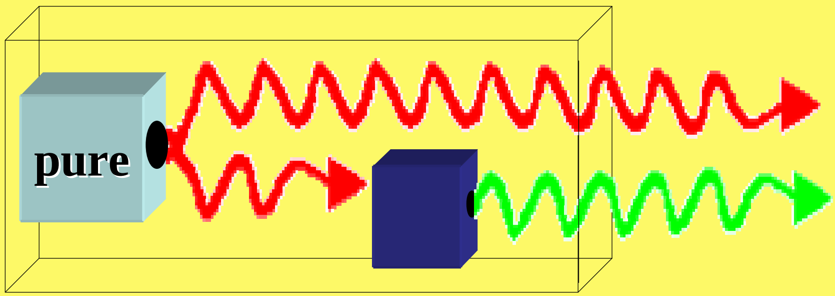


# Entanglement & Capacity

are very closely related

**Theorem:**

Any state ρ can be **decomposed uniquely** as $\rho = (\mathrm{id}\otimes T)(\sigma)$ ,

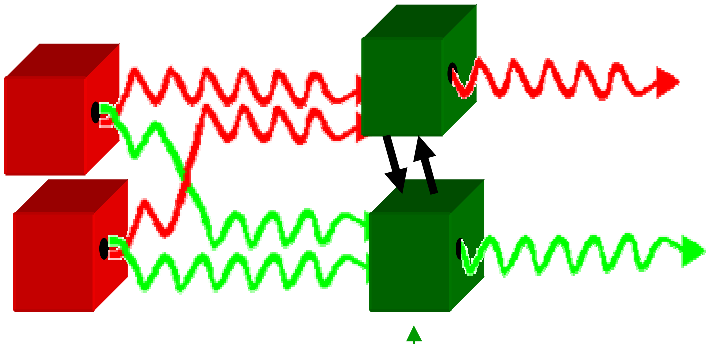



with σ pure and $T$ a channel.

# Entanglement & Capacity

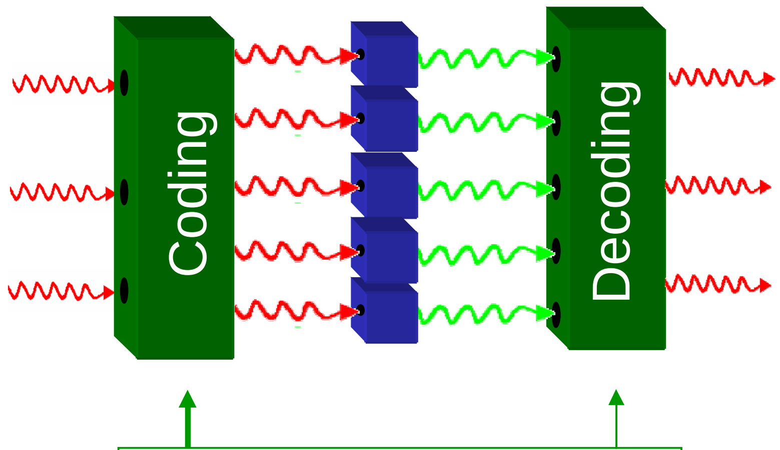
can be upgraded by

## Distillation



Local quantum Operations
&Classical Communication
(LOCC)

## Error correction




Error Correcting Code

best asymptotic (#outputs/#inputs) @ (error$\rightarrow$0)

**Distillible entanglement** **Capacity**

# Comparison of two channels

$$\Delta(S,T) = \inf_{E,D} \left\| S - ETD \right\|_{cb}$$

$C$ is called an achievable rate for S-information through T, if

$$\Delta\left(S^{\otimes n_a}, T^{\otimes m_a}\right) \to 0 \quad \text{for} \quad \limsup_{a} \frac{n_a}{m_a} \le c$$

$$C(S,T) = \sup\{\text{ achievable rates }\}$$

=capacity

(1) S= ideal classical 1 **bit**-channel

$C(S,T)=C(T)$ classical capacity

(2) S= ideal 1 **qubit**-channel

$C(S,T)=Q(T)$ quantum capacity

(3) S= ideal 1 **qubit**-channel, and coding may use arbitrary amounts of entanglement

$\widetilde{C}(S,T)=V(T)$ entanglement-assisted capacity

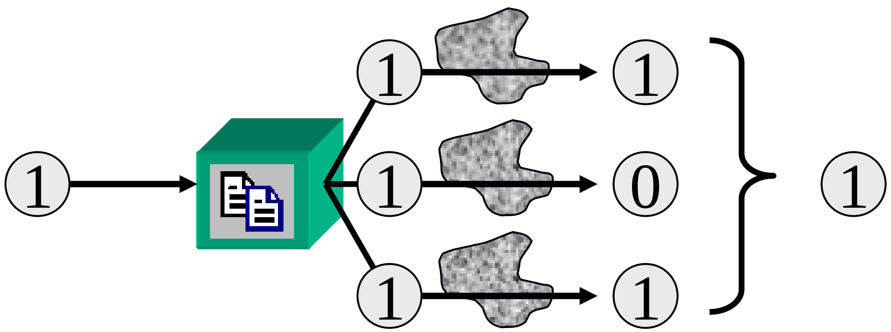
Crucial for all notions of capacity:

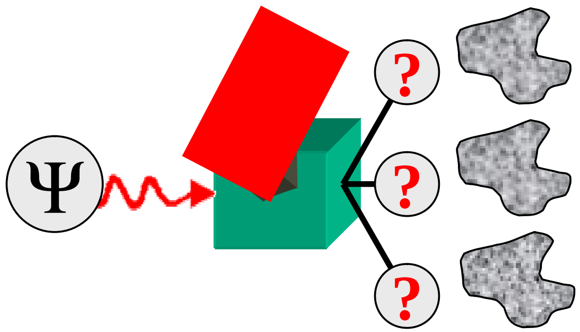
small errors can be corrected

$$\left\| id_d - T \right\|_{cb} \leq \varepsilon \quad \Rightarrow \quad Q(T) \geq (1-\delta)\log_2 d$$

To show this, need good error correcting codes

redundant transmission + majoriy rule
does not work because of No-Cloning Theorem



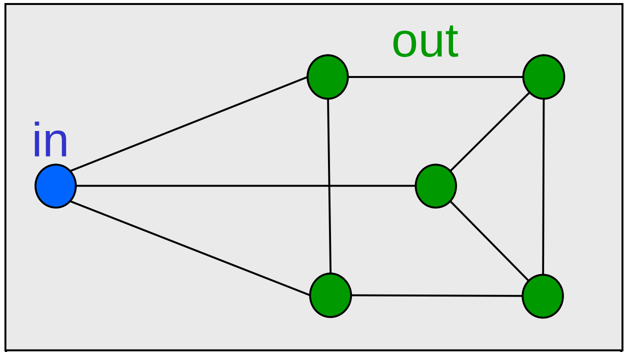
# The best known error correcting codes

- correct a finite number of localized error syndromes and their superpositions.

- This allows the use of algebraic machinery
  (“stabilizer codes“, “Clifford codes“)

- and graphical representation
  (“graph codes“)

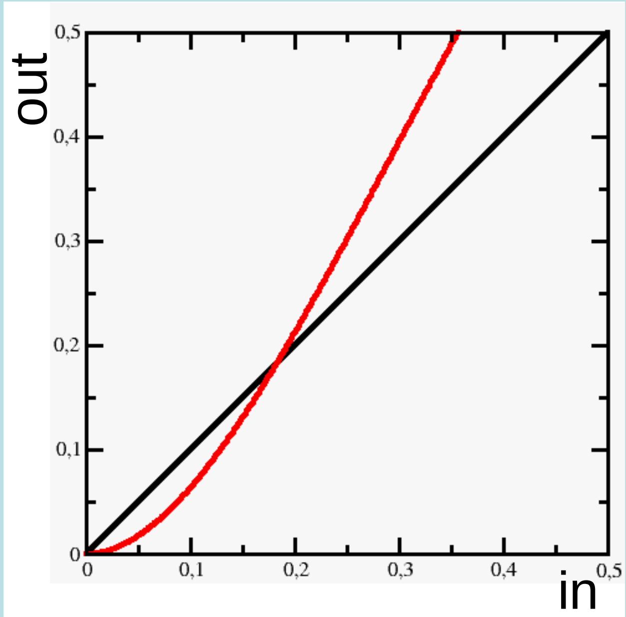
  Codes based on random graphs correct small errors (hashing)




**Five qubit code**
Lines represent phase factors in coding isometry

Problems with this “discrete“ theory of error correcting codes:

- Difficult to optimize for generic given channel
- For finite errors even good codes may be worse than nothing



**Five qubit correction of depolarizing channel**

Find direct optimization procedures without sacred computational basis !

# Open Problems

**http://www.imaph.tu-bs.de/qi/problems**

## (1) Classical capacity:

Do entangled states never ever help to encode classical information?

Then: $C=C_{\text{Holevo}}$, and this quantity is additive.

Hard problem:

- on the decoding side, entanglement may help
- purest outputs of product channels may be for entangled inputs

# Open Problems

QUIPROCONE
Network of Excellence
Q&A Forum

## (2) Quantum capacity $Q$:

### Find Coding Theorem !

(= formula without variation over asymptotically large systems)

Partial Solutions:

- various bounds in examples
- continuity of capacity (small errors)
- connection with entanglement quantities
- Peter Shor (unpublished): $Q$ = regularized coherent information

  Additivity problem as in classical case

# Open Problems

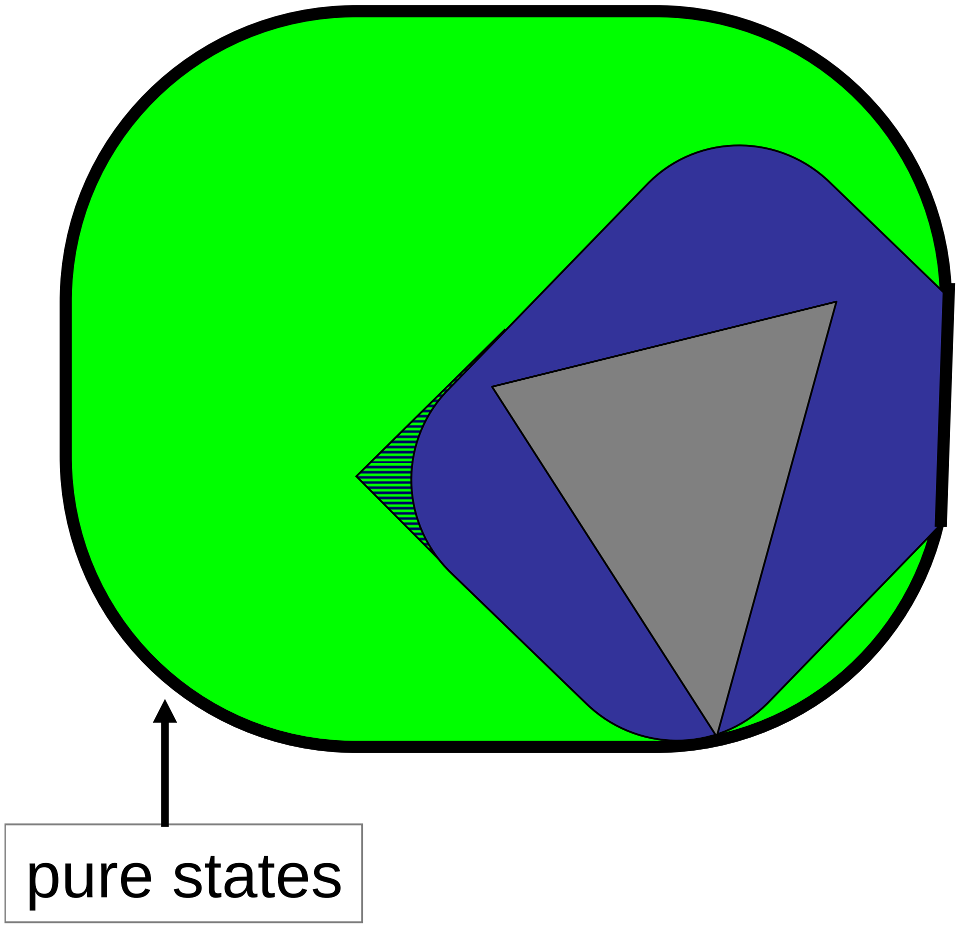
## (3) Entanglement assisted capacity $V$:

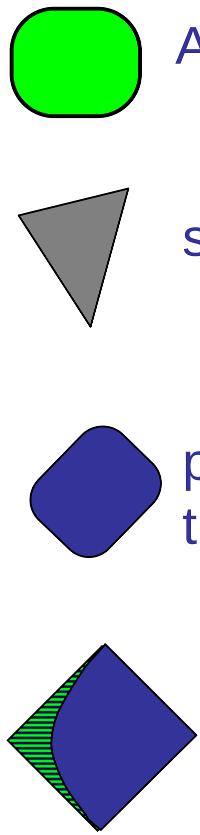
Coding Theorem is proved (Shor, Bennett, Thaplyal),
even with finite entanglement assistance
(Shor, unpublished, up to an additivity problem)

Is this reversible? („Reverse Shannon Theorem")

$$\tilde{C}(S,T)\ \tilde{C}(T,S) = 1$$

# Entanglement (qualitative)



All states of pairs:
≥15 dim convex set

separable states:
Mixtures of products

positive partial
transpose

bound entangled:
not distillable

# Open Problem

Does “non-distillability“ imply “positive partial transpose“ ?

i.e., does the Peres-Horodecki criterion decide distillability rather than entanglement?

Partial Solutions:

- Reduction to a single family of states
- Two papers supporting the conjecture „No“.   (1 US, 1 EQUIP)
- Numerical evidence (untrustworthy)

# Entanglement (quantitative)

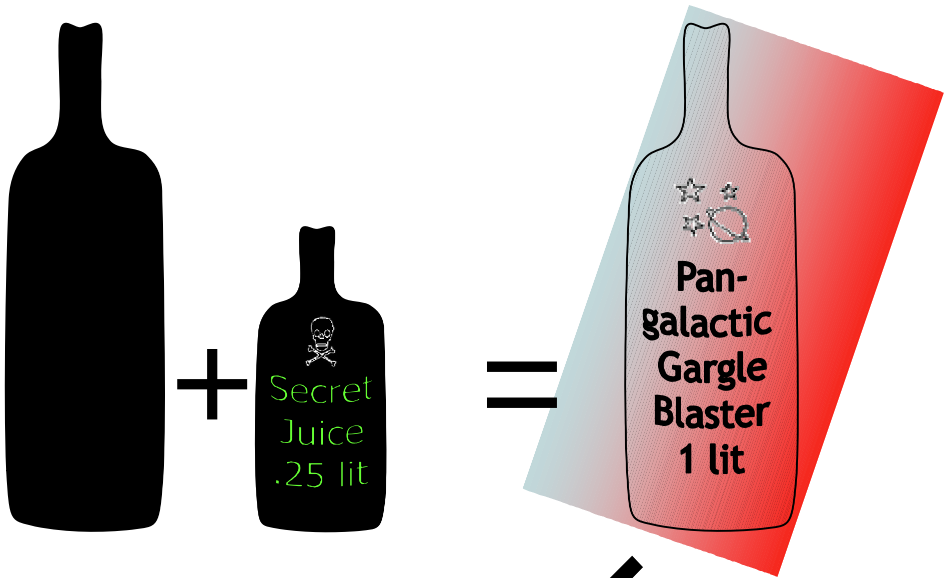
No entanglement measure has been shown to have all the good properties:

positivity, convexity, LOCC-monotonicity, additivity, continuity, computability

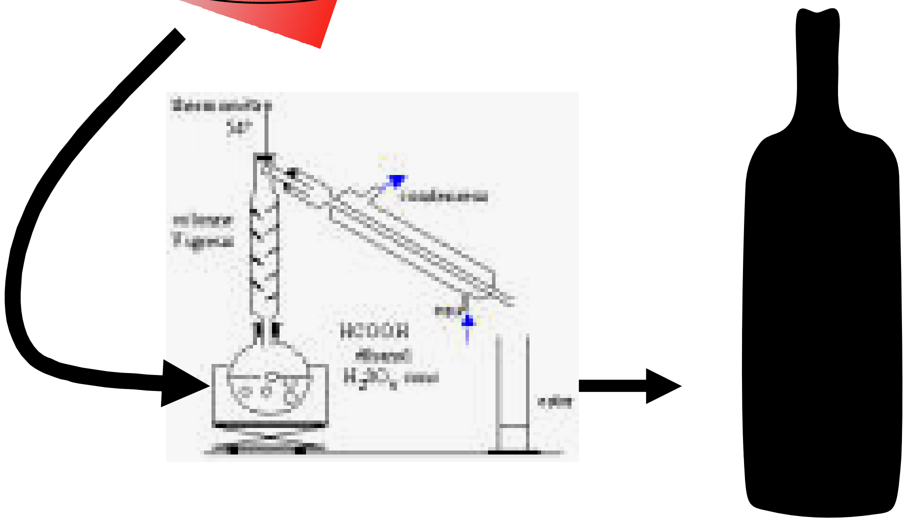
- Distillible entanglement D: how many singlets can I get out?
- Entanglement cost $E_C$: how many singlets do I need? (=regularized entanglement of formation $E_F$)
- Logarithmic negativity $E_N$: additive and computable
- Relative entropy of entanglement $E_R$: makes good bounds

# How much is entanglement like some “stuff“ ?

The distillation metaphor suggests:

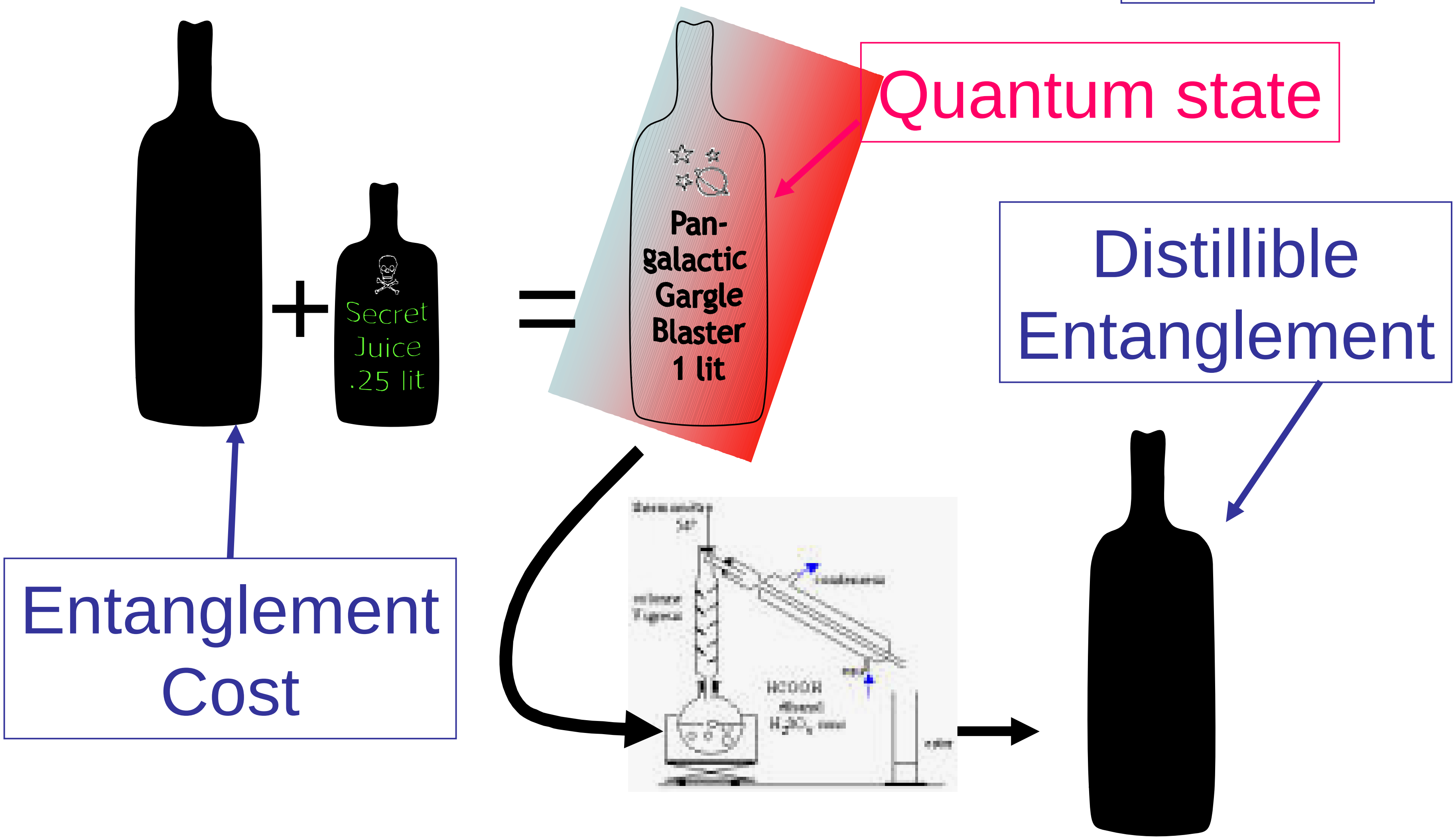



We expect that the alcohol is still there and can be recovered



# How much is entanglement like some “stuff“ ?

The distillation metaphor suggests: $\boxed{E_C = E_D}$



## How much is entanglement like some “stuff“ ?

The distillation metaphor suggests: $\boxed{E_C = E_D}$

- Ok for pure states, and $E_C \geq E_D$ in general.

- But $E_C(\rho) > E_D(\rho)$ for some mixed states ρ. Examples were slow in coming.

- Best example: dim*H*-dimensional family,
  $E_C(\rho) = E_D(\rho)$ in that family iff
  ρ is a locally tagged mixture

## How much is entanglement like some “stuff“ ?

- The distillation metaphor suggests $E_C = E_D$
  but $E_C > E_D$ for most mixed states

- “Stuff“ should be additive with respect to having both pairs : $E(\rho \otimes \sigma) = E(\rho) + E(\sigma)$

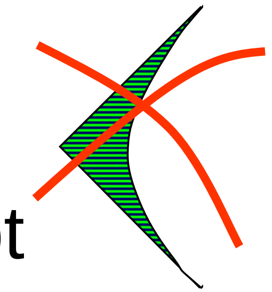
$E_D$ ?  $E_F$ ?  $E_N$ ü  $E_R$ û

# Gaussian states <

- Relevant for quantum optics and collective spin variables

- Parametrized by finite dimensional matrix (although on ∞-dim Hilbert space)

- Existence of bound entangled states, all ppt



- Efficient criterion for separability vs entanglement

# Gaussian states $<$

- Good understanding of required
  “squeezing resources“.

- For some symmetric two mode states:

  computation of $E_F$
  (Gaussian decomposition into Gaussians is optimal!)

  additivity

# Multipartite entanglement

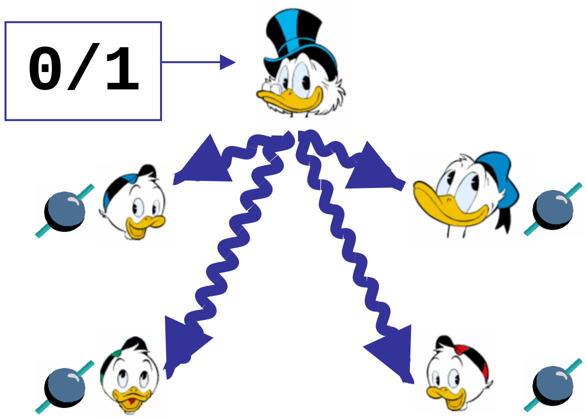
- Many types, even of pure state entanglement including uncomparable ones

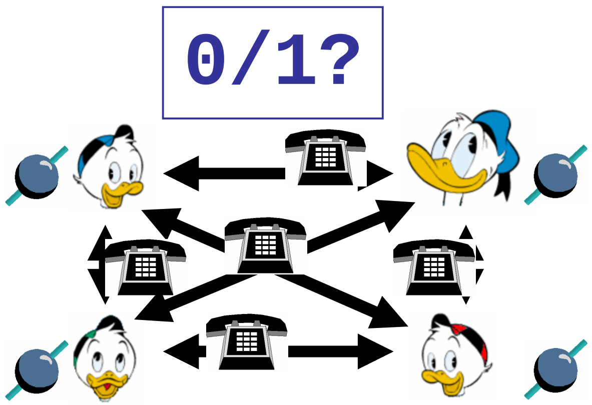
- Complete classification of some symmetric states

- Bell inequalities for many sites, maximal violations thereof

# Multipartite quantum correlations

- Hiding Classical data in multipartite quantum states




Works without entanglement !

- Use of massively multi-partite entanglement in one-way quantum computing.

# Algorithms

Still few …… but no longer embarassingly few

# Shor & descendants

- Variations on Q-Fourier: further signal transforms

- Generalization of period finding:
  hidden subgroup $H \subset G$ :   $f(hg)=f(g)$   $g \in G$, $h \in H$
  works for abelian G and some non-abelian G

- Interesting applications by choice of f:
  Pell´s equation (long history):
  find x,y integers, $x^2 – d\, y^2 = 1$
  Q-algorithm (Hallgren) exponential speedup

- Estimating Gauß sums in finite fields

  still uses Q-Fourier transform

- Quantum random walks

  sometimes hit their target exponentially faster

- A case of Inventor´s paradox

  QI may help to prove classical results

  bounds on locally decodable codes (de Wolf et. al.)

- Fingerprinting

  identify strings by short tag

- Communication complexity:

  set disjointness:

  make appointments with exchange of $\sqrt{N}$ bits

- Classical communication complexity
  in sharper tests of non-locality

# missing ...

- Cryptography

  how not to discard most of the data
  continuous variables
  security against more general attacks

- Simulating Hamiltonians

  given: fixed interaction, local operations
  get: other interactions (cost?)
  also interesting in imaginary time (Stat. Mech.)

-

# Where should we go ? (QI-Theory)

## Continue the quests for ...

The quantitative theory of quantum resources

The Mother of all Additivity Theorems

Better error correcting codes

New algorithmic ideas

New tasks amenable to quantum solution

# Where should we go ? (QI-Theory)

## Look more seriously at ...

Decoherence effects in complex systems

Cellular Automata (very distributed systems)

Statistical mechanics connections

Non-digital coding/computing