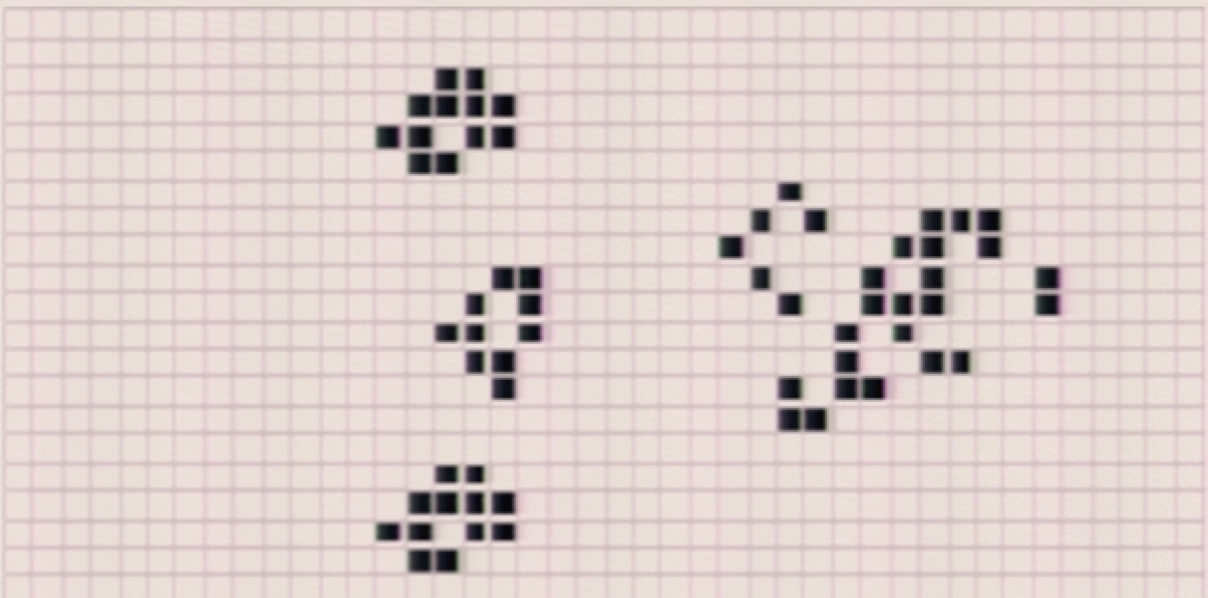
Title: Are Quantum States Exponentially Long Vectors?

Date: Jul 20, 2005 04:15 PM

URL: http://pirsa.org/05070108

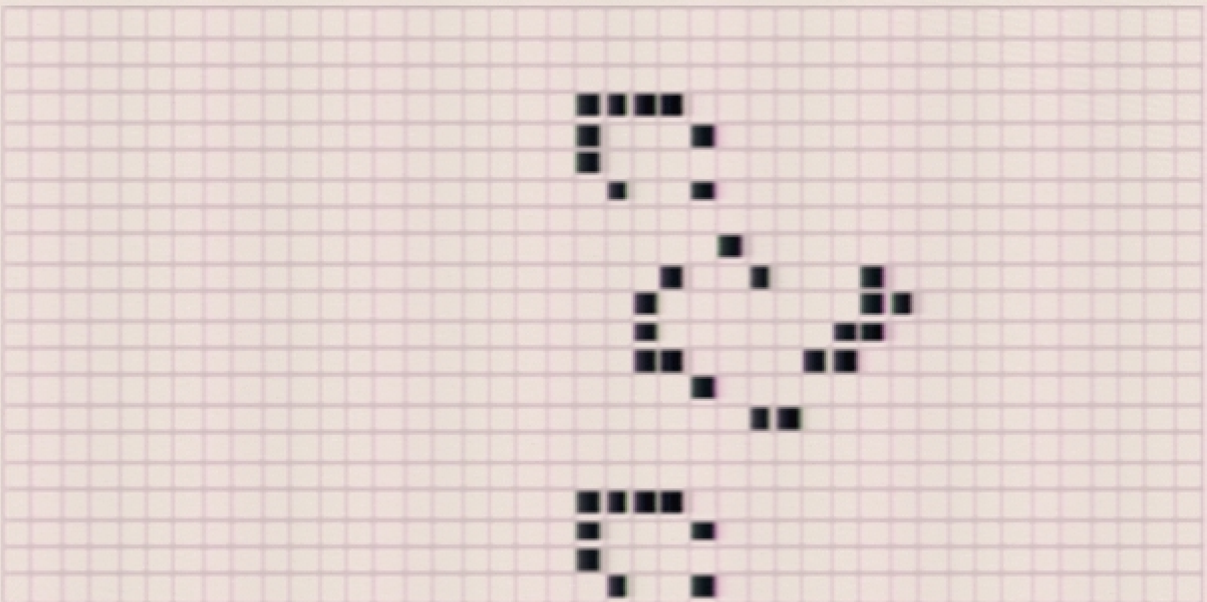
Abstract:

# The Computer Science Picture of Reality



+ details

# The Computer Science Picture of Reality

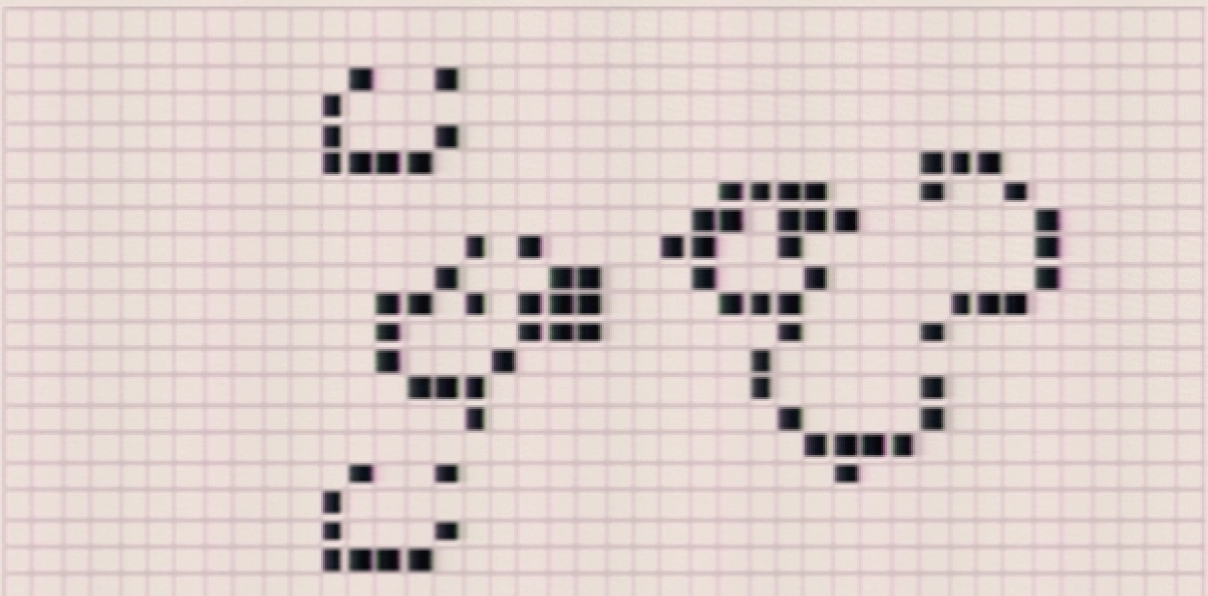


+ details

# The Computer Science Picture of Reality

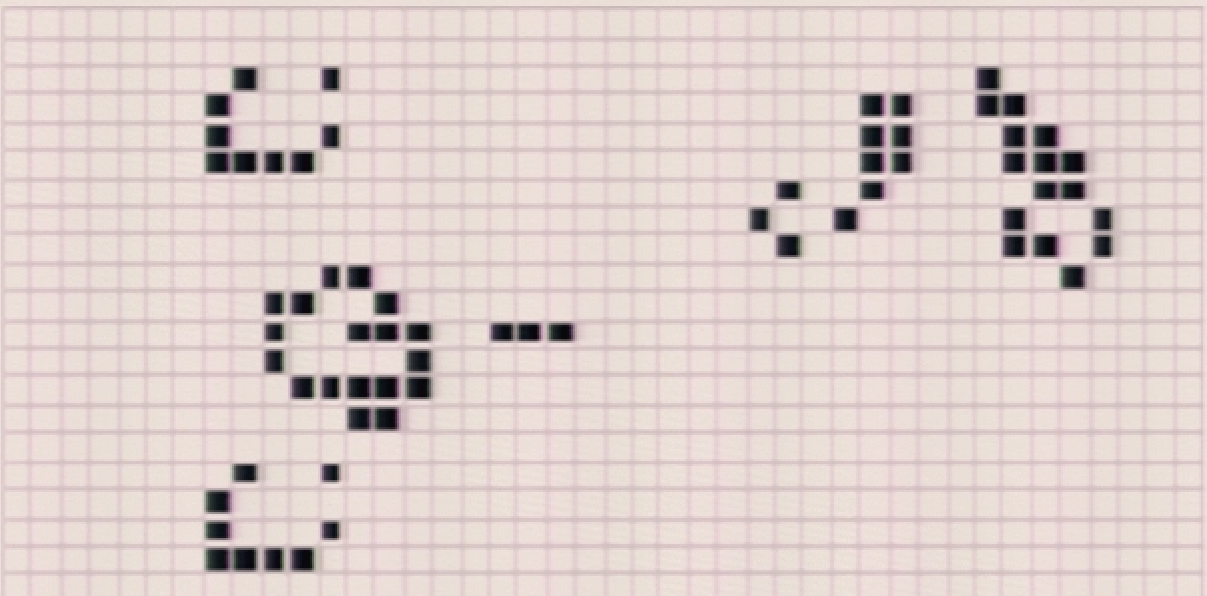
+ details

# The Computer Science Picture of Reality



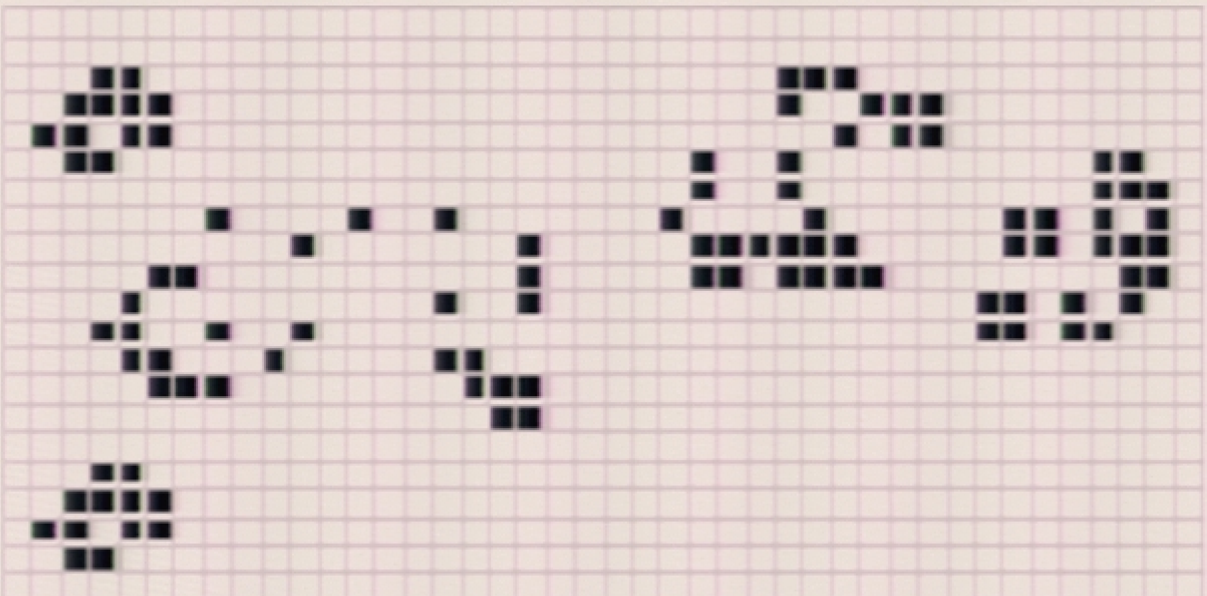
+ details

# The Computer Science Picture of Reality



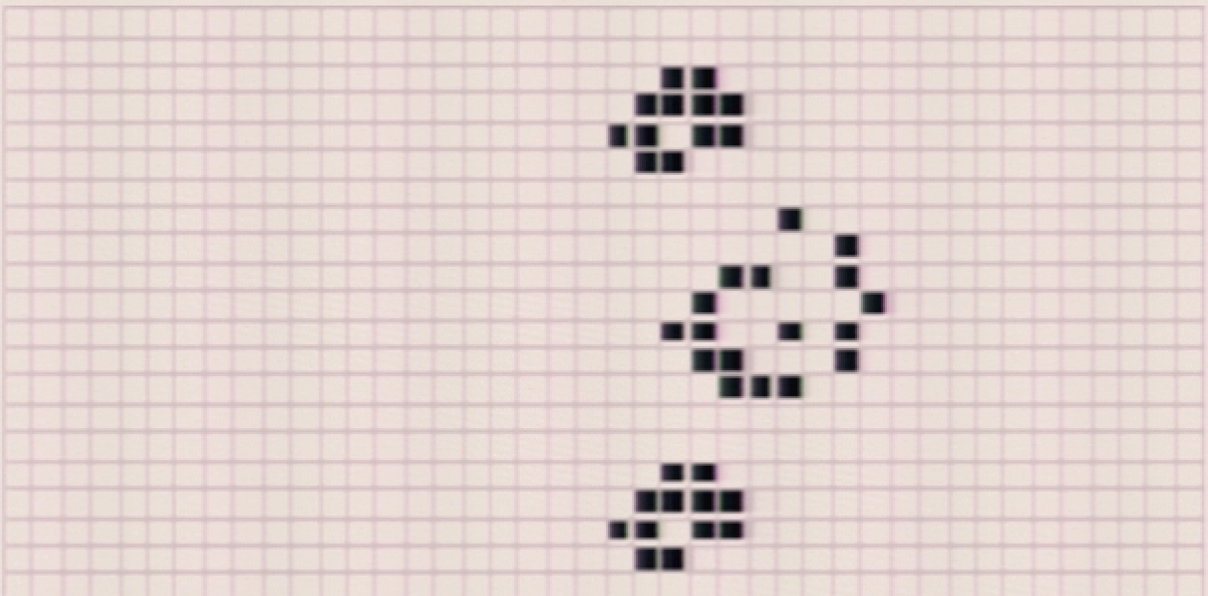
+ details

# The Computer Science Picture of Reality



+ details

# The Computer Science Picture of Reality



+ details

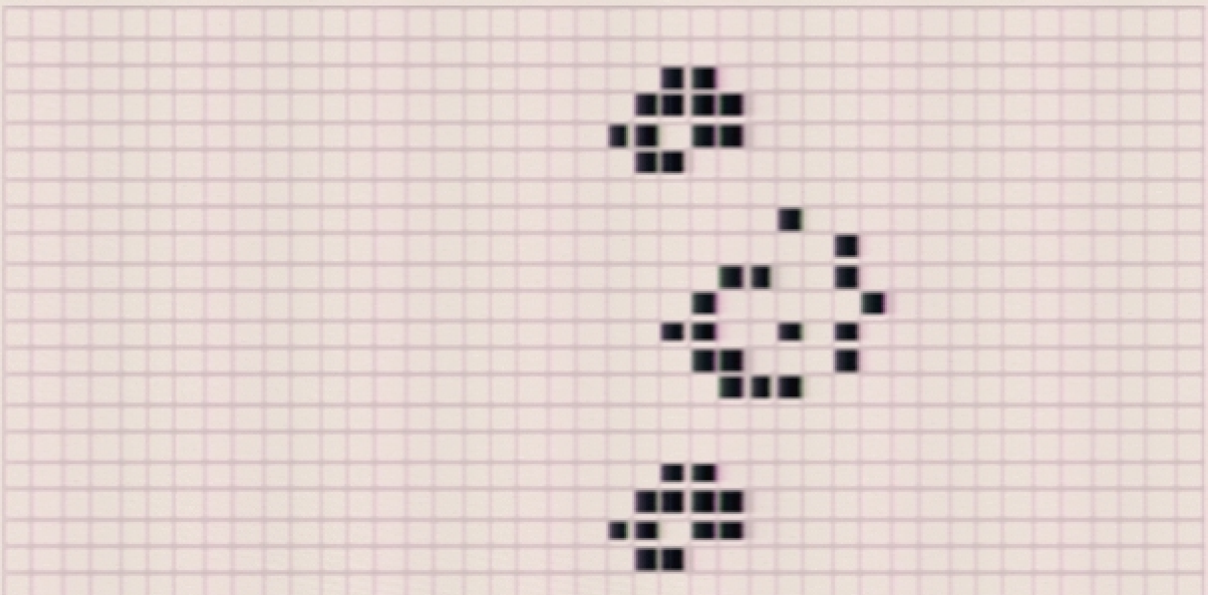
# The Computer Science Picture of Reality

$$\psi$$

Quantum computing challenges this picture

That's why everyone should care about it, whether or not quantum factoring machines are ever built

# The Computer Science Picture of Reality



+ details

As far as I am concern[ed], the QC model consists of exponentially-long vectors (possible configurations) and some “uniform” (or “simple”) operations (computation steps) on such vectors … The key point is that the associated complexity measure postulates that each such operation can be effected at unit cost (or unit time). My main concern is with this postulate. My own intuition is that the cost of such an operation or of maintaining such vectors should be linearly related to the amount of “non-degeneracy” of these vectors, where the “non-degeneracy” may vary from a constant to linear in the length of the vector (depending on the vector). Needless to say, I am not suggesting a concrete definition of “non-degeneracy,” I am merely conjecturing that such exists and that it capture[s] the inherent cost of the computation.

**—Oded Goldreich**

# My Two-Pronged Response

# My Two-Pronged Response

(1) It's not easy to explain current experiments (let alone future ones!), if you don't think that quantum states are exponentially long vectors

[A. 2004, "Multilinear Formulas and Skepticism of Quantum Computing"]

# My Two-Pronged Response

(1) It's not easy to explain current experiments (let alone future ones!), if you don't think that quantum states are exponentially long vectors

[A. 2004, "Multilinear Formulas and Skepticism of Quantum Computing"]

(2) But it's not that bad

[A. 2004, "Limitations of Quantum Advice and One-Way Communication"]

# Prong (1)

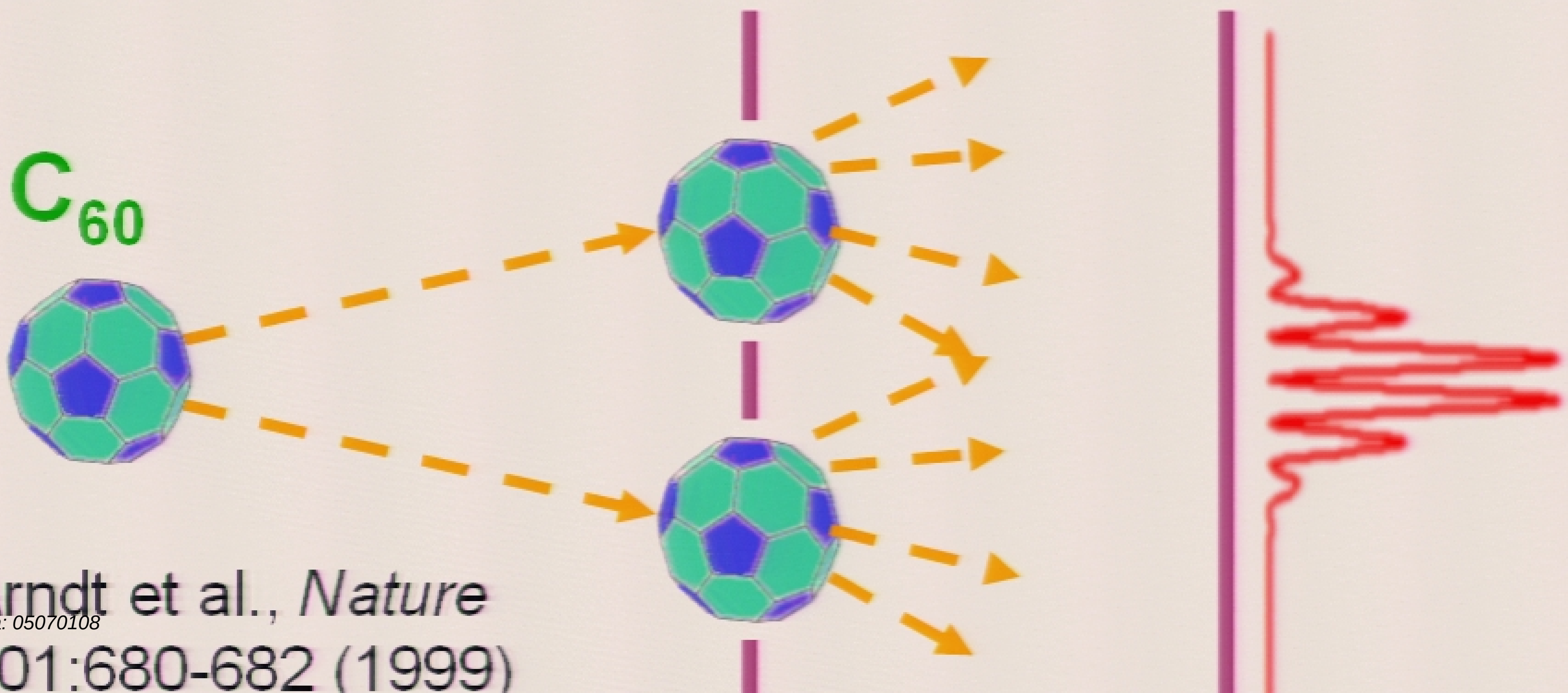
## Quantum states are exponentially long vectors

# How Good Is The Evidence for QM?

**(1) Interference:** Stability of $e^-$ orbits, double-slit, etc.

**(2) Entanglement:** Bell inequality, GHZ experiments

**(3) Schrödinger cats:** $C_{60}$ double-slit experiment, superconductivity, quantum Hall effect, etc.




Arndt et al., *Nature* 401:680-682 (1999)

# Exactly what property separates the Sure States we know we can create, from the Shor States that suffice for factoring?



DIVIDING LINE

Not precision in amplitudes:

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n}$$

Not precision in amplitudes:

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n}$$

Not entanglement across hundreds of particles:

$$\frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}$$

Not precision in amplitudes:

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n}$$

Not entanglement across hundreds of particles:

$$\frac{|0\rangle^{\otimes n}+|1\rangle^{\otimes n}}{\sqrt{2}}$$

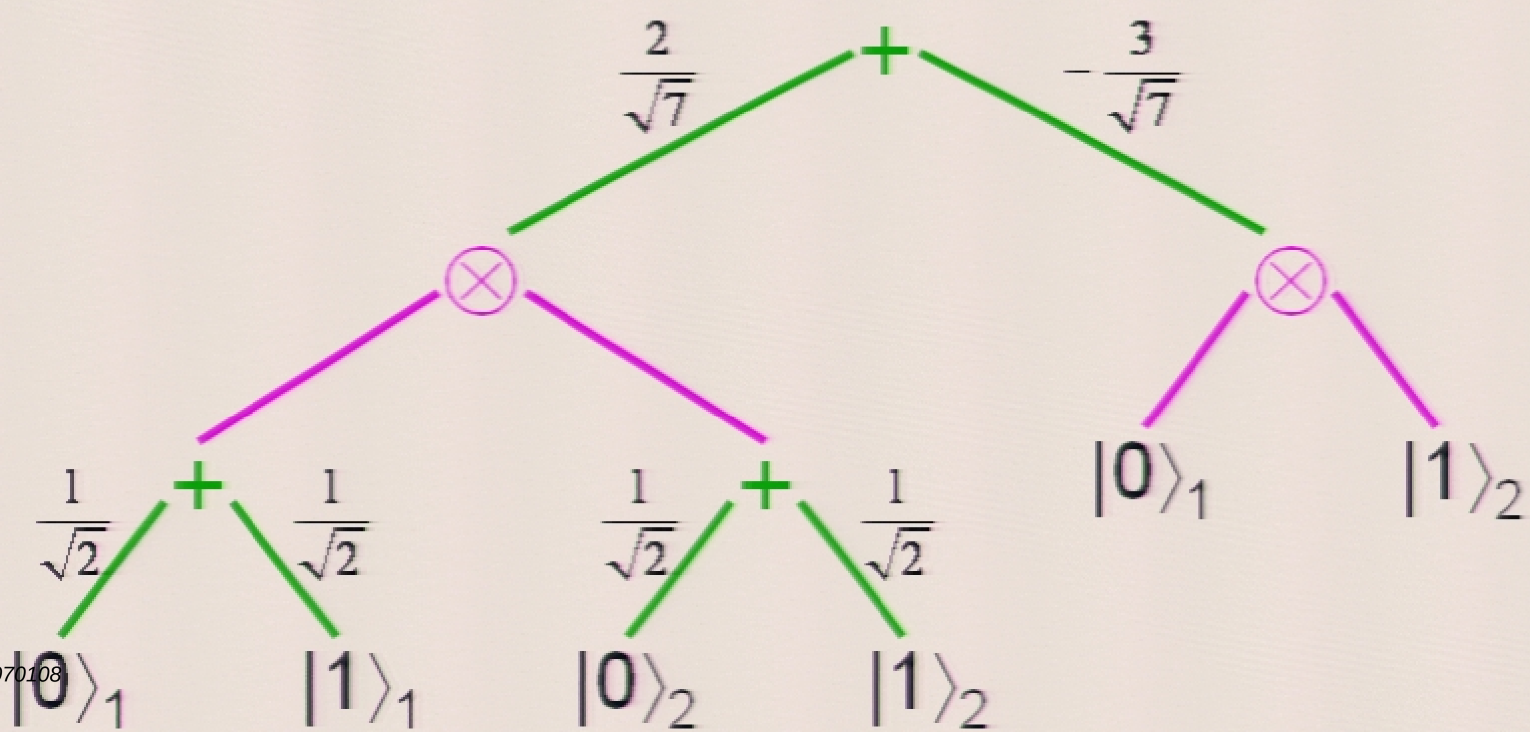
Not a combination of the two:

$$\frac{1}{\sqrt{2}}\left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n}+\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)^{\otimes n}\right]$$

**Intuition:** Once we accept $|\psi\rangle$ and $|\phi\rangle$ into our set of possible states, we're almost **forced** to accept $|\psi\rangle\otimes|\phi\rangle$ and $\alpha|\psi\rangle+\beta|\phi\rangle$ as well

**Intuition:** Once we accept $|\psi\rangle$ and $|\phi\rangle$ into our set of possible states, we're almost **forced** to accept $|\psi\rangle\otimes|\phi\rangle$ and $\alpha|\psi\rangle+\beta|\phi\rangle$ as well

But we might restrict ourselves to **tree states**: n-qubit states obtainable from $|0\rangle$ and $|1\rangle$ by a polynomial number of linear combinations and tensor products



# Main Result

If $|C\rangle = \frac{1}{\sqrt{|C|}} \sum_{x \in C} |x\rangle$ is a uniform superposition over the codewords of a binary linear code, then $|C\rangle$ requires tree size $n^{\Omega(\log n)}$ (even to approximate)—with high probability if the generator matrix is chosen uniformly at random

# Prong (2)

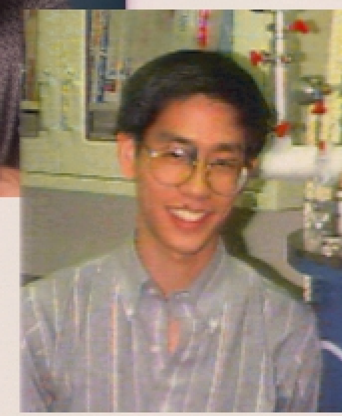
## It's not that bad

# Prong (2)

## It’s not that bad

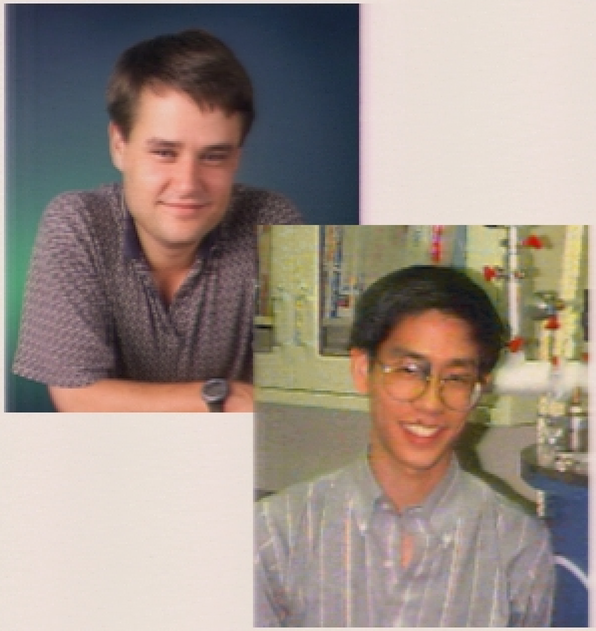
# Quantum Advice

**Nielsen & Chuang:** "We know that many systems in Nature 'prefer' to sit in highly entangled states of many systems; might it be possible to exploit this preference to obtain extra computational power?"



# Quantum Advice

**Nielsen & Chuang:** "We know that many systems in Nature 'prefer' to sit in highly entangled states of many systems; might it be possible to exploit this preference to obtain extra computational power?"



**BQP/qpoly:** Class of languages decidable by polynomial-size, bounded-error quantum circuits, given a polynomial-size **quantum advice state** $|\psi_n\rangle$ that depends only on the input length n

**Challenge:** Is quantum advice more powerful than classical advice?

I.e. does BQP/qpoly strictly contain BQP/poly?

**Challenge:** Is quantum advice more powerful than classical advice?

I.e. does BQP/qpoly strictly contain BQP/poly?

Notice that, given an **exponential** amount of classical advice, a computer could solve any problem whatsoever

So, could quantum advice be similar to that? Could it let us solve, say, NP-complete problems in polynomial time?

**PostBQP:** Class of problems solvable in quantum polynomial time, if you can **postselect** measurement outcomes (i.e. measure, then kill yourself if you don't like the outcome)

**A. 2004:** PostBQP equals a classical complexity class called PP

**PostBQP:** Class of problems solvable in quantum polynomial time, if you can **postselect** measurement outcomes (i.e. measure, then kill yourself if you don't like the outcome)

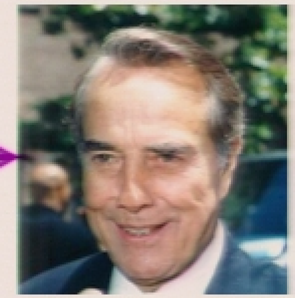
**A. 2004:** PostBQP equals a classical complexity class called PP

**Result:** **BQP/qpoly $\subseteq$ PostBQP/poly**

(Anything you can do with poly-size quantum advice, you can also do with poly-size *classical* advice, provided you're willing to use exponentially more computation time)

# Intuition

Alice is the "advisor"

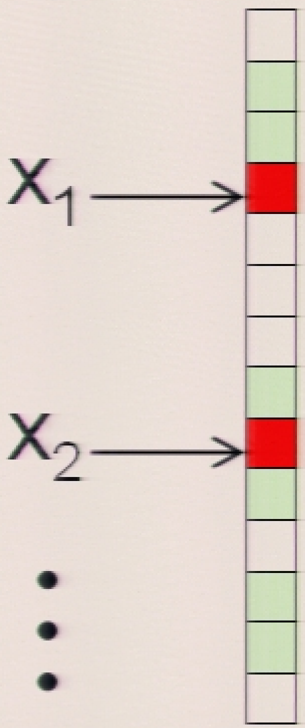


Bob is the PostBQP machine

Alice wanted to send Bob a Q-qubit quantum advice state $|\psi\rangle$

Instead she'll send Bob an O(nQ)-qubit **classical** message, containing a "Darwinian training set" of inputs that he can use to reconstruct $|\psi\rangle$ on his own

# Alice's Classical Message




**Bob,** if you use the maximally mixed state in place of my quantum message, then $x_1$ is the lexicographically first input for which you'll output the wrong answer with probability at least 1/3.

But if you condition on succeeding on $x_1$, then $x_2$ is the next input for which you'll output the wrong answer with probability at least 1/3.

But if you condition on succeeding on $x_1$ *and* $x_2$, then $x_3$ is the …

**Technicality:** We assume Alice's quantum message was boosted, so that the error probability is negligible

**Technicality:** We assume Alice's quantum message was boosted, so that the error probability is negligible

**Claim:** Alice only needs to send T=O(Q) inputs $x_1,\ldots,x_T$

**Proof Sketch:** Bob succeeds on $x_1,\ldots,x_T$ simultaneously with probability at most $(2/3)^T$.

But we can decompose the Q-qubit maximally mixed state as $\frac{1}{2^Q}\sum_{i=1}^{2^Q}|\psi_i\rangle\langle\psi_i|$ where $|\psi_1\rangle=|\psi\rangle$ is Alice's "true" quantum message. Therefore Bob succeeds with probability $\Omega(1/2^Q)$

# Recent Improvement:

## BQP/qpoly $\subseteq$ QMA/poly

Here QMA (Quantum Merlin-Arthur) is the quantum generalization of NP: the class of problems for which a "yes" answer can be proven with a polynomial-size quantum witness

(Note that QMA $\subseteq$ PostBQP)

# Recent Improvement:

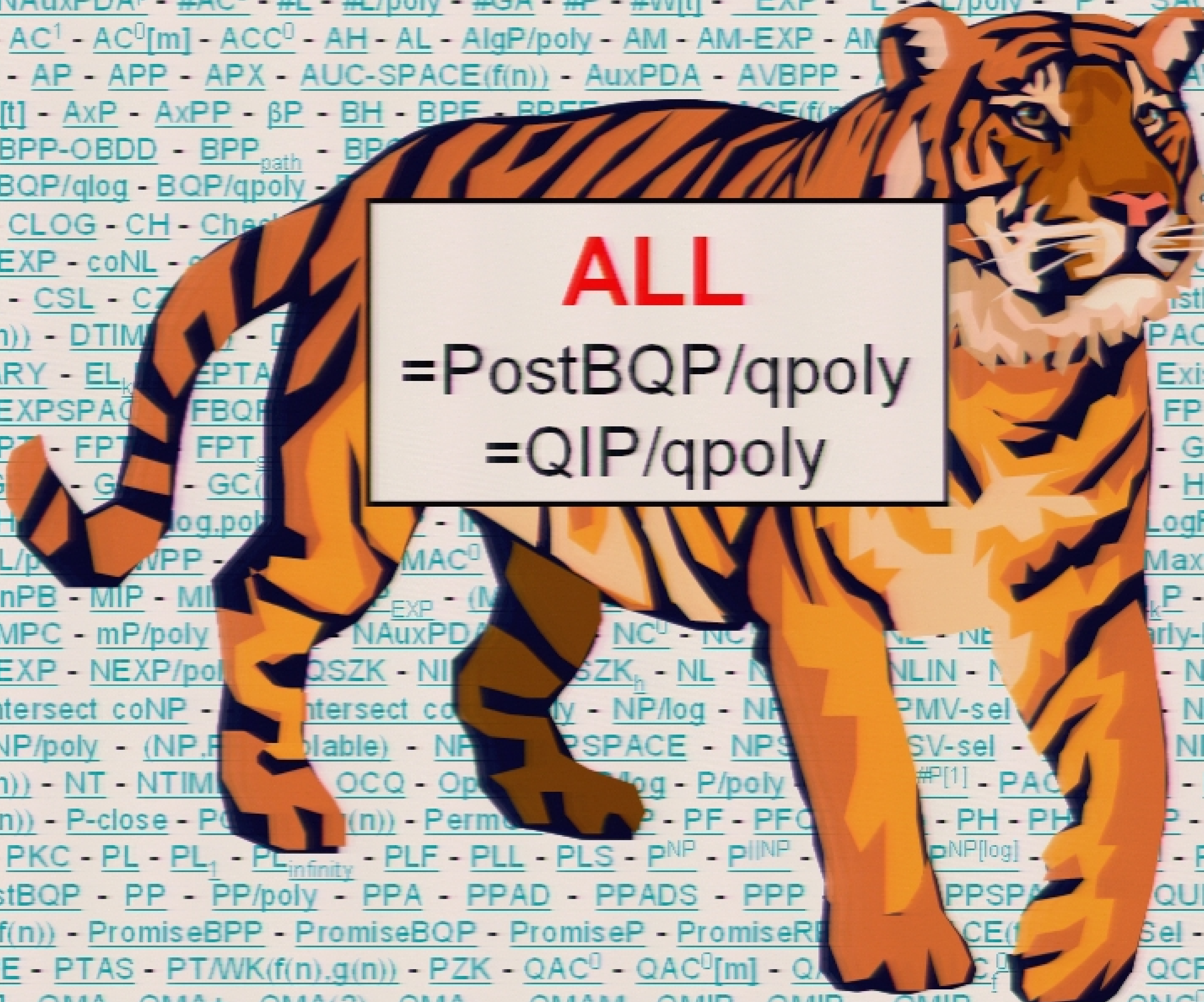
## BQP/qpoly $\subseteq$ QMA/poly

Here QMA (Quantum Merlin-Arthur) is the quantum generalization of NP: the class of problems for which a "yes" answer can be proven with a polynomial-size quantum witness

(Note that QMA $\subseteq$ PostBQP)

**Yet another improvement:**
QCMA/qpoly $\subseteq$ QMA/poly, where QCMA (Quantum Classical Merlin-Arthur) is the generalization of NP with a *quantum* verifier but a *classical* witness

0-1-$NP_C$ - 1NAuxPDA$^p$ - #$AC^0$ - #L - #L/poly - #GA - #P - #W[t] - EXP - L - L/poly - P - $SAC^0$ - $SAC^1$ - $A_0PP$ - AC - $AC^0$ - $AC^1$ - $AC^0$[m] - $ACC^0$ - AH - AL - AlgP/poly - AM - AM-EXP - AM intersect coAM - AM[polylog] - AmpMP - AmpP-BQP - AP - APP - APX - AUC-SPACE(f(n)) - AuxPDA - AVBPP - AvE - AvP - AW[P] - AWPP - AW[SAT] - AW[*] - AW[t] - AxP - AxPP - βP - BH - BPE - BPEE - $BP_H$SPACE(f(n)) - BPL - BP•NP - BPP - $BPP^{cc}$ - $BPP^{KT}$ - BPP//log - BPP-OBDD - $BPP_{path}$ - BPQP - BPSPACE(f(n)) - BPTIME(f(n)) - BQNC - BQNP - BQP - BQP/log - BQP/poly - BQP/qlog - BQP/qpoly - BQP-OBDD - BQPSPACE - $BQP_{tt}$/poly - BQTIME(f(n)) - k-BWBP - C_$AC^0$ - C_L - C_P - CFL - CLOG - CH - Check - $C_kP$ - CNP - coAM - coC_P - cofrIP - Coh - coMA - $coMod_kP$ - compIP - compNP - coNE - coNEXP - coNL - coNP - $coNP^{cc}$ - coNP/poly - coNQP - coRE - coRNC - coRP - coSL - coUCC - coUP - CP - CSIZE(f(n)) - CSL - CZK - D#P - DCFL - $\Delta_2P$ - δ-BPP - δ-RP - DET - Diff$AC^0$ - DisNP - DistNP - DP - DQP - DSPACE(f(n)) - DTIME(f(n)) - DTISP(t(n),s(n)) - Dyn-FO - Dyn-Th$C^0$ - E - EE - EEE - EESPACE - EEXP - EH - ELEMENTARY - $EL_kP$ - EPTAS - k-EQBP - EQP - EQTIME(f(n)) - ESPACE - ExistsBPP - ExistsNISZK - EXP - EXP/poly - EXPSPACE - FBQP - Few - FewP - FH - FNL - FNL/poly - FNP - FO(t(n)) - FOLL - FP - $FP^{NP[log]}$ - FPR - FPRAS - FPT - $FPT_{nu}$ - $FPT_{su}$ - FPTAS - FQMA - frIP - F-TAPE(f(n)) - F-TIME(f(n)) - GA - GAN-SPACE(f(n)) - Gap$AC^0$ - GapL - GapP - GC(s(n),C) - GCSL - GI - GLO - GPCD(r(n),q(n)) - G[t] - HeurBPP - HeurBPTIME(f(n)) - $H_kP$ - HP - HVSZK - IC[log,poly] - IP - IPP - IP[polylog] - L - LIN - $L_kP$ - LOGCFL - LogFew - LogFewNL - LOGNP - LOGSNP - L/poly - LWPP - MA - MA' - $MAC^0$ - MA-E - MA-EXP - mAL - MaxNP - MaxPB - MaxSNP - $MaxSNP^0$ - mcoNL - MinPB - MIP - MIP*[2,1] - $MIP_{EXP}$ - $(M_k)P$ - mL - $mNC^1$ - mNL - mNP - $Mod_kL$ - $Mod_kP$ - ModP - $ModZ_kL$ - mP - MP - MPC - mP/poly - $mTC^0$ - NAuxPDA$^p$ - NC - $NC^0$ - $NC^1$ - $NC^2$ - NE - NE/poly - Nearly-P - NEE - NEEE - NEEXP - NEXP - NEXP/poly - NIQSZK - NISZK - $NISZK_h$ - NL - NL/poly - NLIN - NLOG - NP - NPC - $NP^{cc}$ - $NP_C$ - NPI - NP intersect coNP - (NP intersect coNP)/poly - NP/log - NPMV - NPMV-sel - $NPMV_t$ - $NPMV_t$-sel - NPO - NPOPB - NP/poly - (NP,P-samplable) - $NP_R$ - NPSPACE - NPSV - NPSV-sel - $NPSV_t$ - $NPSV_t$-sel - NQP - NSPACE(f(n)) - NT - NTIME(f(n)) - OCQ - OptP - P - P/log - P/poly - $P^{\#P}$ - $P^{\#P[1]}$ - $PAC^0$ - PBP - k-PBP - $P_C$ - $P^{cc}$ - PCD(r(n),q(n)) - P-close - PCP(r(n),q(n)) - PermUP - PEXP - PF - PFCHK(t(n)) - PH - $PH^{cc}$ - $\Phi_2P$ - PhP - $\Pi_2P$ - PINC - PIO - $P^K$ - PKC - PL - $PL_1$ - $PL_{infinity}$ - PLF - PLL - PLS - $P^{NP}$ - $P^{||NP}$ - $P^{NP[k]}$ - $P^{NP[log]}$ - $P^{NP[log^2]}$ - P-OBDD - PODN - polyL - PostBQP - PP - PP/poly - PPA - PPAD - PPADS - PPP - $P^{PP}$ - PPSPACE - PQUERY - PR - $P_R$ - $Pr_H$SPACE(f(n)) - PromiseBPP - PromiseBQP - PromiseP - PromiseRP - PrSPACE(f(n)) - P-Sel - PSK - PSPACE - $PT_1$ - PTAPE - PTAS - PT/WK(f(n),g(n)) - PZK - $QAC^0$ - $QAC^0$[m] - $QACC^0$ - $QAC_f^0$ - QAM - QCFL - QCMA - QH - QIP - QIP[2] - QMA - QMA+ - QMA(2) - $QMA_{log}$ - QMAM - QMIP - $QMIP_{le}$ - $QMIP_{ne}$ - QNC - $QNC^0$ - $QNC_f^0$ - $QNC^1$ - QP - QPLIN - QPSPACE - QRG - $QS_2P$ - QSZK - R - RE - REG - RevSPACE(f(n)) - RG - RG(1) - $R_HL$ - $R_H$SPACE(f(n)) - RL - RNC - RP - RPP - RSPACE(f(n)) - $S_2P$ - $S_2$-EXP•$P^{NP}$ - SAC - $SAC^0$ - $SAC^1$ - SAPTIME - SBP - SC - SE - SEH - SelfNP - $SF_k$ - $\Sigma_2P$ - SKC - SL - SLICEWISE PSPACE - SNP - SO-E - SP - SP - span-P - SPARSE - SPL - SPP - SQG - SUBEXP - symP - SZK - $SZK_h$ - TALLY - $TC^0$ - TFNP - $\Theta_2P$ - TreeBQP - TREE-REGULAR - UAP - UCC - UE - UL - UL/poly - UP - US - $VNC_k$ - $VNP_k$ - $VP_k$ - $VQP_k$ - W[1] - WAPP - W[P] - WPP - W[SAT] - W[*] - W[t]

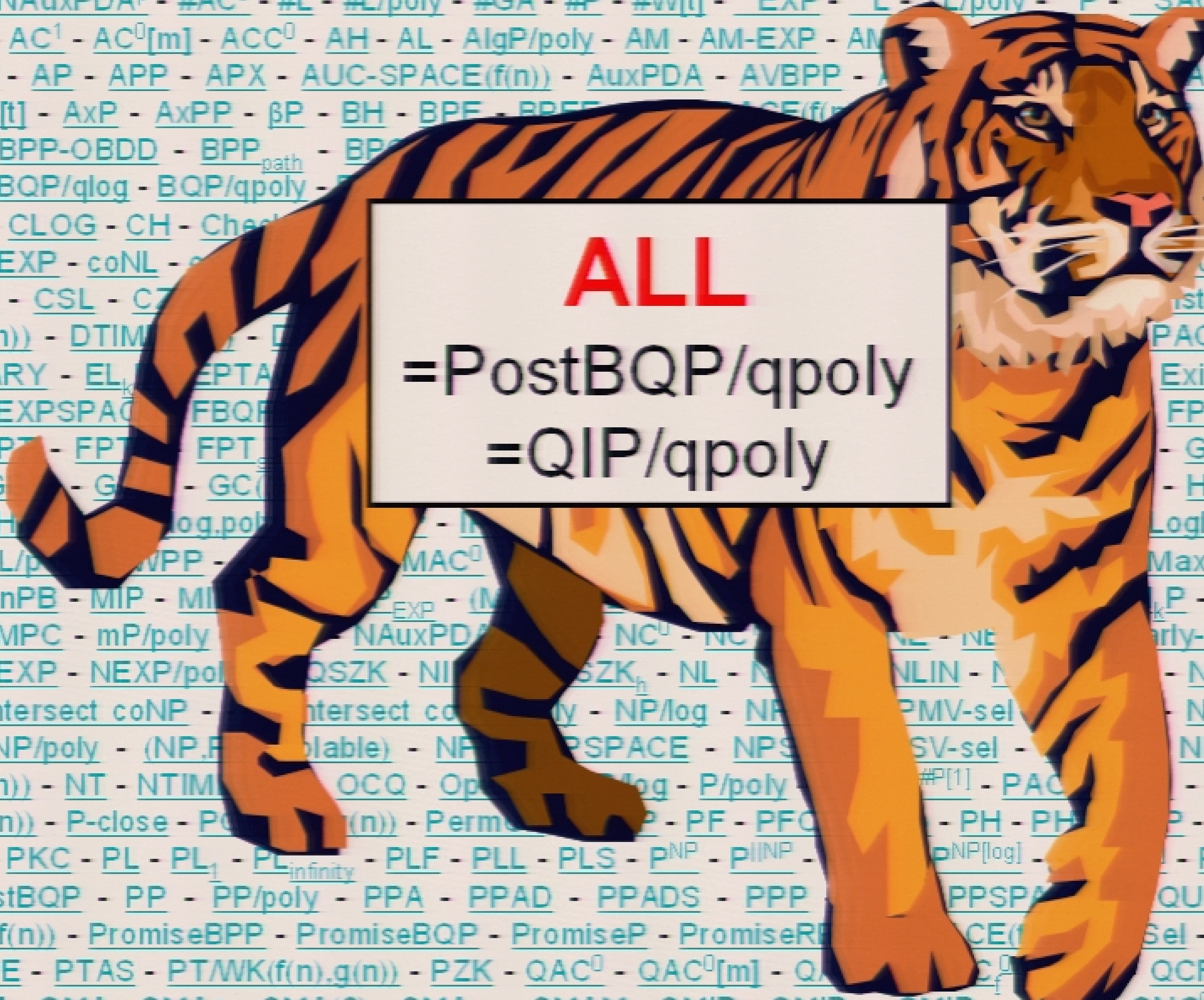


# ALL

=PostBQP/qpoly

=QIP/qpoly


ALL
=PostBQP/qpoly
=QIP/qpoly

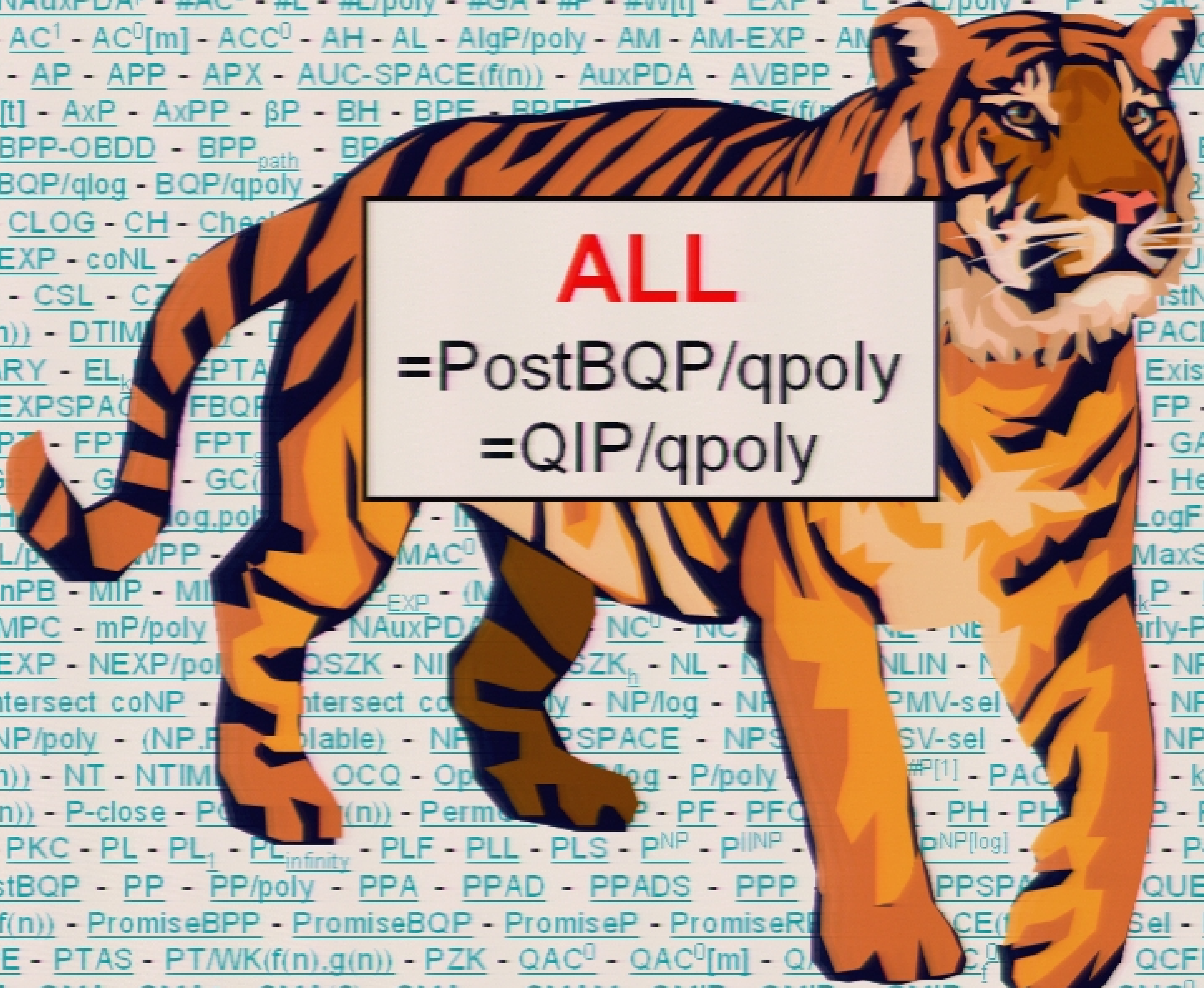


# ALL
=PostBQP/qpoly
=QIP/qpoly

**The good news:** This tiger seems to have nothing to do with quantum computing

# Conjectures

- ALL can be quarantined—in particular, QMA/qpoly $\subseteq$ PostBQP/poly



**ALL**

=PostBQP/qpoly

=QIP/qpoly

**The good news:** This tiger seems to have nothing to do with quantum computing

# Conjectures

- ALL can be quarantined—in particular, QMA/qpoly $\subseteq$ PostBQP/poly

# Conjectures

- ALL can be quarantined—in particular, QMA/qpoly $\subseteq$ PostBQP/poly
- The question of whether classical advice can always replace quantum advice is not independent of ZF set theory

# Conjectures

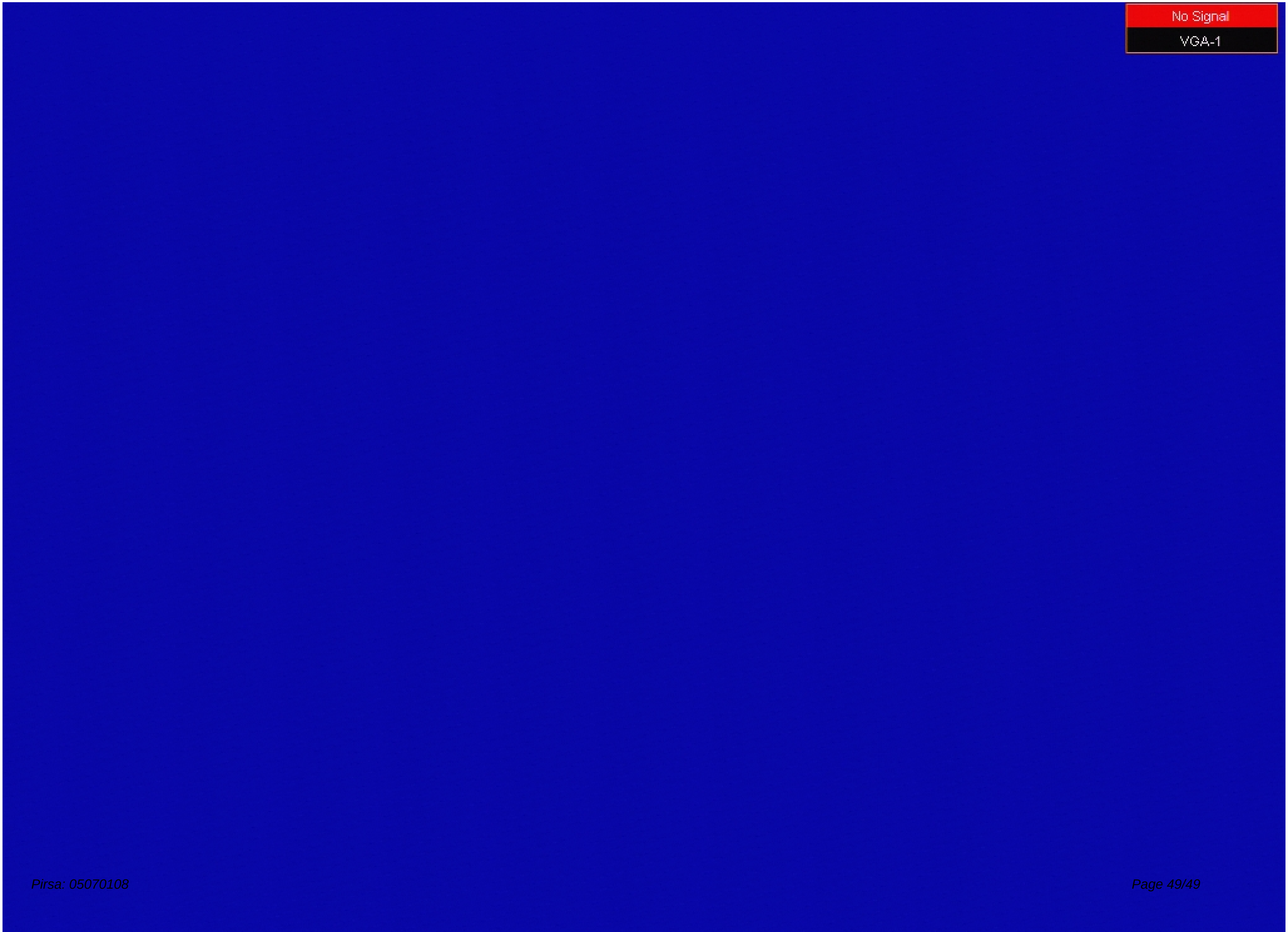
- ALL can be quarantined—in particular, QMA/qpoly $\subseteq$ PostBQP/poly
- The question of whether classical advice can always replace quantum advice is not independent of ZF set theory
- Similarly for whether classical proofs can replace quantum proofs (i.e. QCMA = QMA)

# Summary

• The state of n particles is an exponentially long vector.  Welcome to Quantum World!

# Summary

- The state of n particles is an exponentially long vector. Welcome to Quantum World!
- But for most complexity-theoretic purposes, it's no worse than a **probability distribution** being an exponentially long vector


No Signal
VGA-1