Noncontextuality violation as a robust quantum resource

Matthew F. Pusey
Perimeter Institute
joint work with Mike Mazurek, Ravi Kunjwal,
Rob Spekkens, and Kevin Resch

January 11th, 2016

Preparation Contextuality Powers Parity-Oblivious Multiplexing

Robert W. Spekkens,[1] D. H. Buzacott,[2,3] A. J. Keehn,[2,3] Ben Toner,[4] and G. J. Pryde[2,3]

[1]*DAMTP, University of Cambridge, Cambridge, CB3 0WA, United Kingdom*
[2]*Centre for Quantum Computer Technology, Griffith University, Brisbane 4111, Australia*
[3]*Centre for Quantum Dynamics, Griffith University, Brisbane 4111, Australia*
[4]*Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands*

(Received 12 May 2008; published 5 January 2009)

In a noncontextual hidden variable model of quantum theory, hidden variables determine the outcomes of every measurement in a manner that is independent of how the measurement is implemented. Using a generalization of this notion to arbitrary operational theories and to preparation procedures, we demonstrate that a particular two-party information-processing task, "parity-oblivious multiplexing," is powered by contextuality in the sense that there is a limit to how well any theory described by a noncontextual hidden variable model can perform. This bound constitutes a "noncontextuality inequality" that is violated by quantum theory. We report an experimental violation of this inequality in good agreement with the quantum predictions. The experimental results also provide the first demonstration of 2-to-1 and 3-to-1 quantum random access codes.

DOI: 10.1103/PhysRevLett.102.010401 PACS numbers: 03.65.Ta, 03.67.−a, 42.50.Dv, 42.50.Ex

The Bell-Kochen-Specker theorem [1] shows that the

The NC inequality we derive provides a bound on the

PRL **102,** 010401 (2009) PHYSICAL REVIEW LETTERS week ending 9 JANUARY 2009

Preparation Contextuality Powers Parity-Oblivious Multiplexing

Robert W. Spekkens,[1] D. H. Buzacott,[2,3] A. J. Keehn,[2,3] Ben Toner,[4] and G. J. Pryde[2,3]

PHYSICAL REVIEW A **88**, 022322 (2013)

Contextuality in measurement-based quantum computation

Robert Raussendorf*

Department of Physics and Astronomy, University of British Columbia, Vancouver, British Columbia V6T 1Z1, Canada

(Received 1 May 2013; revised manuscript received 11 July 2013; published 19 August 2013)

We show, under natural assumptions for qubit systems, that measurement-based quantum computations (MBQCs) which compute a nonlinear Boolean function with a high probability are contextual. The class of contextual MBQCs includes an example which is of practical interest and has a superpolynomial speedup over the best-known classical algorithm, namely, the quantum algorithm that solves the "discrete log" problem.

DOI: 10.1103/PhysRevA.88.022322 PACS number(s): 03.67.Ac, 03.65.Ta

I. INTRODUCTION

While numerous quantum algorithms have been found that offer polynomial or superpolynomial speedups over their classical counterparts [1–3], the precise quantum mechanical origin of this speedup remains unknown. The prominent candidates—entanglement [4], superposition and interference [5], and largeness of Hilbert space—provide an intuitive understanding in many situations. Yet, as a whole, the

discuss experimental tests of contextuality. We conclude with a discussion in Sec. V.

II. THE SETTING

We discuss the link between contextuality and quantum computation for MBQC [15]. MBQC is a model of quantum computation in which a quantum algorithm is implemented solely by local measurements on a fixed initial state. The

PRL 102, 010401 (2009) PHYSICAL REVIEW LETTERS week ending 9 JANUARY 2009

Preparation Contextuality Powers Parity-Oblivious Multiplexing

Robert W. Spekkens,[1] D. H. Buzacott,[2,3] A. J. Keehn,[2,3] Ben Toner,[4] and G. J. Pryde[2,3]

PHYSICAL REVIEW A 88, 022322 (2013)

Contextuality in measurement-based quantum computation

Robert Raussendorf*

ARTICLE

doi:10.1038/nature13460

Contextuality supplies the ‘magic’ for quantum computation

Mark Howard[1,2], Joel Wallman[2], Victor Veitch[2,3] & Joseph Emerson[2]

Quantum computers promise dramatic advantages over their classical counterparts, but the source of the power in quantum computing has remained elusive. Here we prove a remarkable equivalence between the onset of contextuality and the possibility of universal quantum computation via ‘magic state’ distillation, which is the leading model for experimentally realizing a fault-tolerant quantum computer. This is a conceptually satisfying link, because contextuality, which precludes a simple ‘hidden variable’ model of quantum mechanics, provides one of the fundamental characterizations of uniquely quantum phenomena. Furthermore, this connection suggests a unifying paradigm for the resources of quantum information: the non-locality of quantum theory is a particular kind of contextuality, and non-locality is already known to be a critical resource for achieving advantages with quantum communication. In addition to clarifying these fundamental issues, this work advances the resource framework for quantum computation, which has a number of practical applications, such as characterizing the efficiency and trade-offs between distinct theoretical and experimental schemes

PRL **102,** 010401 (2009) PHYSICAL REVIEW LETTERS week ending 9 JANUARY 2009

Preparation Contextuality Powers Parity-Oblivious Multiplexing

Robert W. Spekkens,[1] D. H. Buzacott,[2,3] A. J. Keehn,[2,3] Ben Toner,[4] and G. J. Pryde[2,3]

PHYSICAL REVIEW A **88**, 022322 (2013)

Contextuality in measurement-based quantum computation

Robert Raussendorf*

ARTICLE

doi:10.1038/nature13460

PHYSICAL REVIEW X **5,** 021003 (2015)

Wigner Function Negativity and Contextuality in Quantum Computation on Rebits

Nicolas Delfosse,[1] Philippe Allard Guerin,[2] Jacob Bian,[2] and Robert Raussendorf[2]

[1]*Département de Physique, Université de Sherbrooke, Sherbrooke, Québec, J1K 2R1, Canada*

[2]*Department of Physics and Astronomy, University of British Columbia, Vancouver, British Columbia V6T 1Z1, Canada*

(Received 1 October 2014; published 2 April 2015)

We describe a universal scheme of quantum computation by state injection on rebits (states with real density matrices). For this scheme, we establish contextuality and Wigner function negativity as computational resources, extending results of M. Howard *et al.* [Nature (London) 510, 351 (2014)] to two-level systems. For this purpose, we define a Wigner function suited to systems of n rebits and prove a corresponding discrete Hudson's theorem. We introduce contextuality witnesses for rebit states and discuss the compatibility of our result with state-independent contextuality.

DOI: 10.1103/PhysRevX.5.021003 Subject Areas: Quantum Physics, Quantum Information

I. INTRODUCTION

In quantum computation by state injection (QCSI) [1], the set of quantum gates is, by construction, not universal. This restriction is compensated by the injection of states

QCSI since the restricted gate set therein is typically chosen to be the Clifford gates. These gates are indeed not universal, and—if supplemented only with Pauli measurements and stabilizer states—can be efficiently classically simulated by stabilizer techniques.

PRL 102, 010401 (2009) PHYSICAL REVIEW LETTERS week ending 9 JANUARY 2009

Preparation Contextuality Powers Parity-Oblivious Multiplexing

Robert W. Spekkens,[1] D. H. Buzacott,[2,3] A. J. Keehn,[2,3] Ben Toner,[4] and G. J. Pryde[2,3]

PHYSICAL REVIEW A 88, 022322 (2013)

Contextuality in measurement-based quantum computation

Robert Raussendorf*

ARTICLE

doi:10.1038/nature13460

PHYSICAL REVIEW X 5, 021003 (2015)

Wigner Function Negativity and Contextuality in Quantum Computation on Rebits

Nicolas Delfosse,[1] Philippe Allard Guerin,[2] Jacob Bian,[2] and Robert Raussendorf[2]
[1]*Départment de Physique, Université de Sherbrooke, Sherbrooke, Québec, J1K 2R1, Canada*
[2]*Department of Physics and Astronomy, University of British Columbia, Vancouver,*

Contextuality as a resource for qubit quantum computation

Robert Raussendorf[1], Dan E. Browne[2], Nicolas Delfosse[3,4,5], Cihan Okay[6], Juan Bermejo-Vega[7,8]

1: Department of Physics and Astronomy, University of British Columbia, Vancouver, BC, Canada,
2: Department of Physics and Astronomy, University College London, Gower Street, London, UK,
3: Département de Physique, Université de Sherbrooke, Sherbrooke, Québec, Canada,
4: IQIM, California Institute of Technology, Pasadena, CA, USA,
5: Department of Physics and Astronomy, University of California, Riverside, California, 92521, USA,
6: Department of Mathematics, University of Western Ontario, London, Ontario, Canada,
7: Max-Planck Institut für Quantum Optics, Theory Division, Garching, Germany,
8: Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, Berlin, Germany

(Dated: November 30, 2015)

We describe a scheme of quantum computation with magic states on qubits for which contextuality is a necessary resource possessed by the magic states. More generally, we establish contextuality as a necessary resource for all schemes of quantum computation with magic states on qubits that satisfy three simple postulates. Furthermore, we identify stringent consistency conditions on such

Part I

Introduction to contextuality

Ontological models

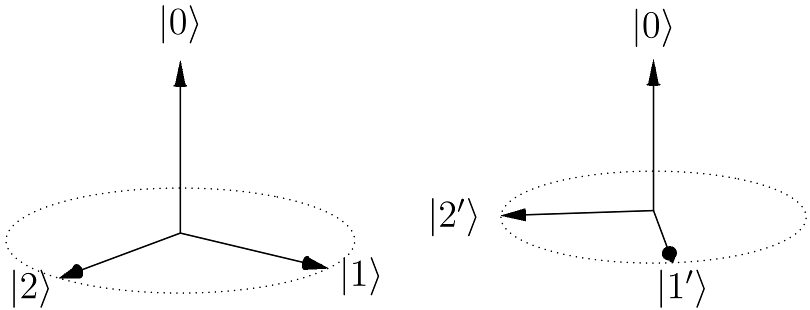
$$p(k|\mathcal{P},\mathcal{M}) = \int p(k|\lambda,\mathcal{M})p(\lambda|\mathcal{P})d\lambda$$

Kochen-Specker noncontextuality

$$p(k|\lambda, \mathcal{M}) = v(\Pi_k) \in \{0, 1\}$$

Kochen-Specker noncontextuality

$$p(k|\lambda, \mathcal{M}) = v(\Pi_k) \in \{0, 1\}$$



Operational measurment noncontextuality[1]

$$p(k|\mathcal{P},\mathcal{M}) = p(k|\mathcal{P},\mathcal{M}') \; \forall \mathcal{P}$$

$$\Downarrow$$

$$p(k|\lambda,\mathcal{M}) = p(k|\lambda,\mathcal{M}') \; \forall \lambda$$

[1] R.W. Spekkens, PRA **71**, 052108

Preparation noncontextuality

$$p(k|\mathcal{P},\mathcal{M}) = p(k|\mathcal{P}',\mathcal{M}) \ \forall k,\mathcal{M}$$

$$\Downarrow$$

$$p(\lambda|\mathcal{P}) = p(\lambda|\mathcal{P}') \ \forall \lambda$$

Example of preparation noncontextuality

$$\frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{|+\rangle\langle +| + |-\rangle\langle -|}{2}$$

Example of preparation noncontextuality

$$\frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{|+\rangle\langle +| + |-\rangle\langle -|}{2}$$

$$\Downarrow$$

$$\frac{p(\lambda|\,|0\rangle) + p(\lambda|\,|1\rangle)}{2} = \frac{p(\lambda|\,|+\rangle) + p(\lambda|\,|-\rangle)}{2}$$

Part II

Robustness

Operational $\implies$ robust?

$$p(k|\mathcal{P},\mathcal{M}) = p(k|\mathcal{P}',\mathcal{M}) \;\forall k,\mathcal{M}$$

$$\Downarrow$$

$$p(\lambda|\mathcal{P}) = p(\lambda|\mathcal{P}') \;\forall \lambda$$

Operational = robust?

$$p(k|\mathcal{P},\mathcal{M}) = p(k|\mathcal{P}',\mathcal{M}) \ \forall k,\mathcal{M}$$

$$\Downarrow$$

$$p(\lambda|\mathcal{P}) = p(\lambda|\mathcal{P}') \ \forall \lambda$$

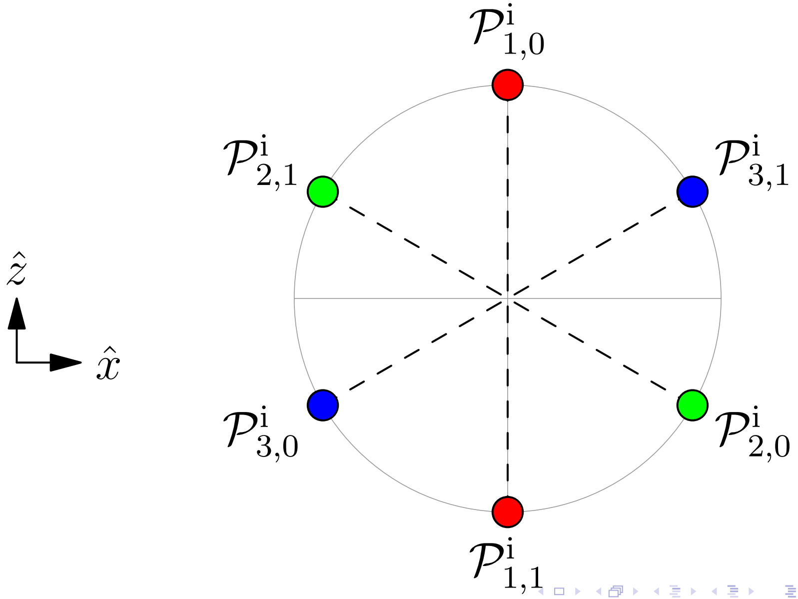
Operational = robust?

$$p(k|\mathcal{P},\mathcal{M}) = p(k|\mathcal{P}',\mathcal{M})\ \forall k,\mathcal{M}$$

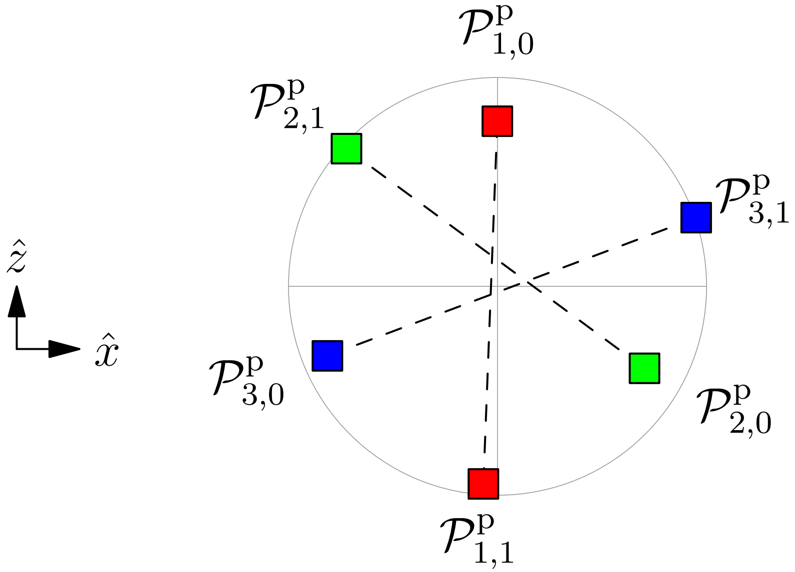
$$\Downarrow$$

$$p(\lambda|\mathcal{P}) = p(\lambda|\mathcal{P}')\ \forall\lambda$$

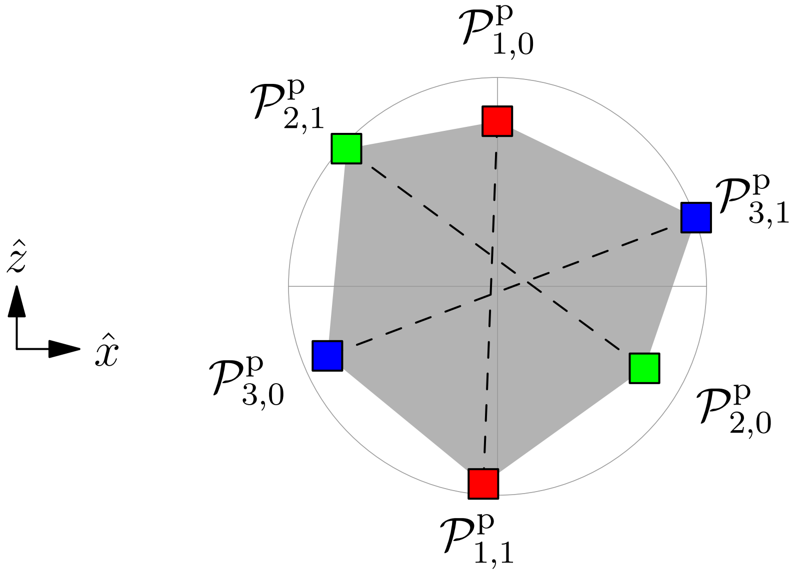
Ideal case


$\mathcal{P}^{\mathrm{i}}_{1,0}$
$\mathcal{P}^{\mathrm{i}}_{2,1}$
$\mathcal{P}^{\mathrm{i}}_{3,1}$
$\hat{z}$
$\hat{x}$
$\mathcal{P}^{\mathrm{i}}_{3,0}$
$\mathcal{P}^{\mathrm{i}}_{2,0}$
$\mathcal{P}^{\mathrm{i}}_{1,1}$

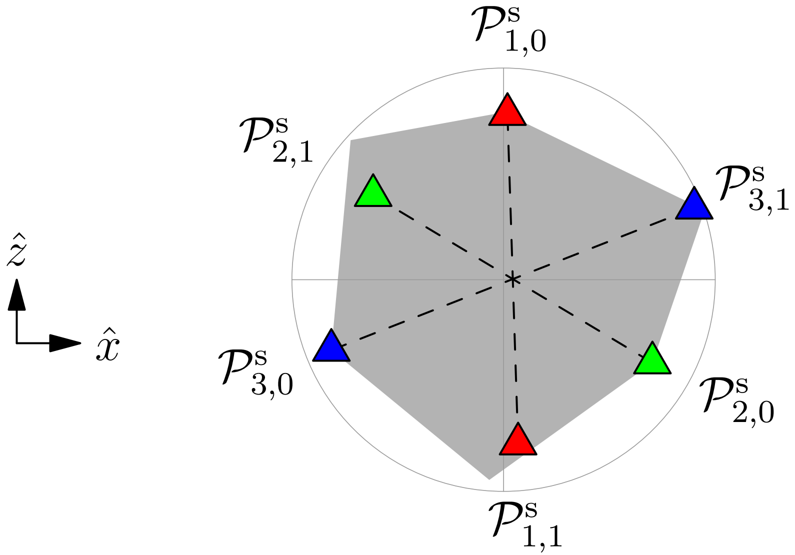
Imperfect case



Secondary preparations



Secondary preparations



Projective measurements

Operational signature: perfect predictability

$$\forall k \; \exists \mathcal{P}_k \text{ s.t. } p(k|\mathcal{P}_k, \mathcal{M}) = 1$$

Projective measurements

Operational signature: perfect predictability

$$\forall k \; \exists \mathcal{P}_k \text{ s.t. } p(k|\mathcal{P}_k, \mathcal{M}) = 1$$

Ontological reflection: determinism

$$p(k|\lambda, \mathcal{M}) \in \{0, 1\}$$

Nearly projective measurements

Operational signature: high predictability

$$\forall k \; \exists \mathcal{P}_k \text{ s.t. } p(k|\mathcal{P}_k, \mathcal{M}) \geq 1 - \epsilon$$

Nearly projective measurements

Operational signature: high predictability

$$\forall k \; \exists \mathcal{P}_k \text{ s.t. } p(k|\mathcal{P}_k, \mathcal{M}) \geq 1 - \epsilon$$

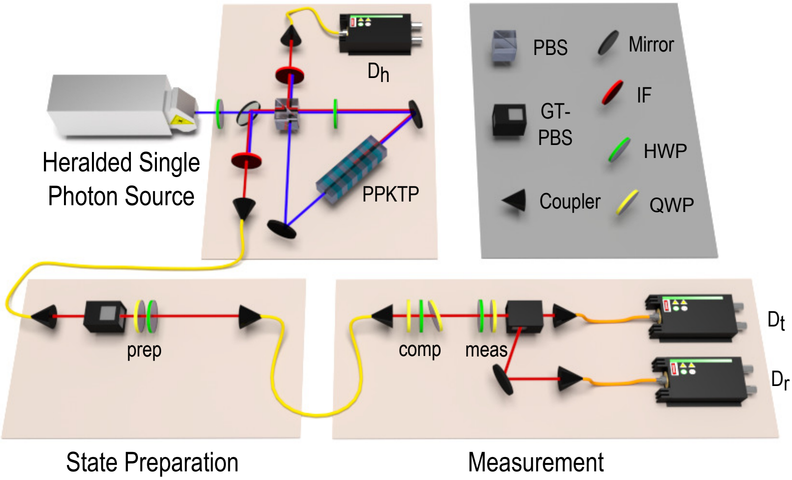
Ontological reflection: near-determinism

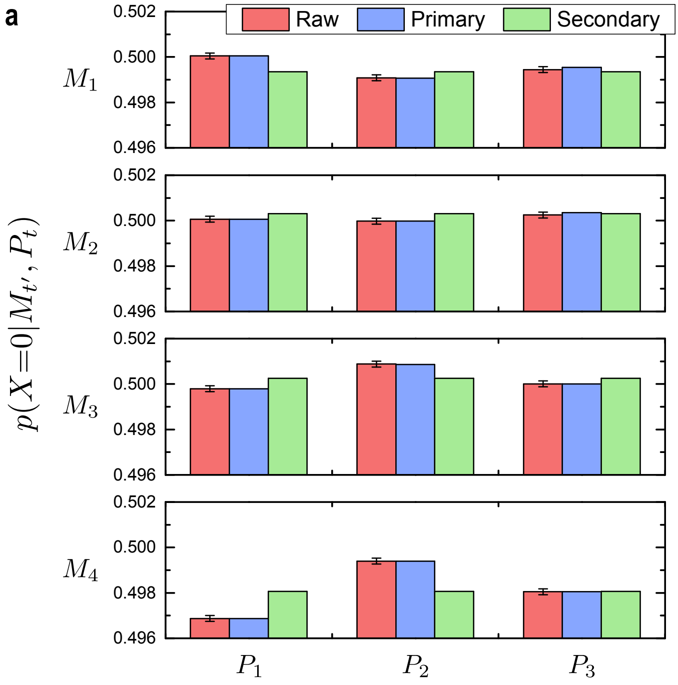
$$\max_{\lambda,k} p(k|\lambda, \mathcal{M}) \geq 1 - \epsilon$$

Part III

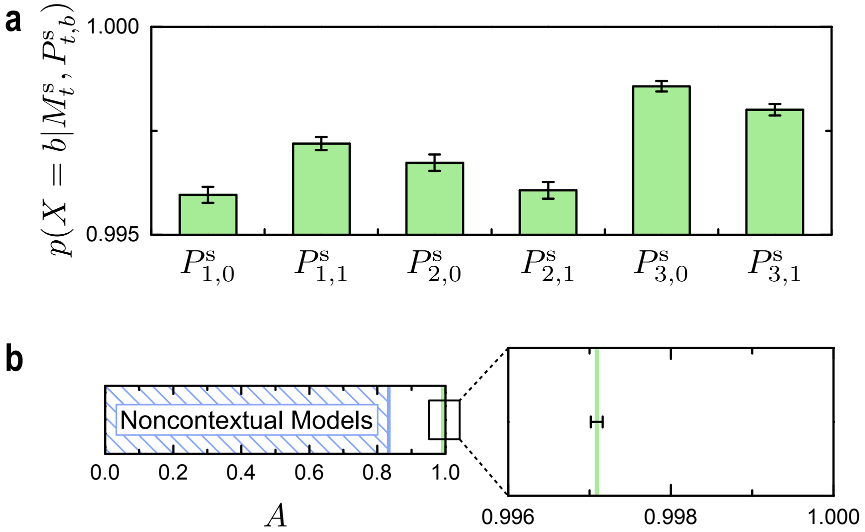
Our experiment

Setup


Dh
Heralded Single
Photon Source
PPKTP
PBS
Mirror
GT-
PBS
IF
HWP
Coupler
QWP
Dt
Dr
prep
comp
meas
State Preparation
Measurement



a
Raw
Primary
Secondary
$p(X=0|M_{t'}, P_t)$
M_1
M_2
M_3
M_4
0.502
0.500
0.498
0.496
P_1
P_2
P_3


a
$p(X=b|M_t^{\mathrm{s}}, P_{t,b}^{\mathrm{s}})$
1.000
0.995
$P_{1,0}^{\mathrm{s}}$
$P_{1,1}^{\mathrm{s}}$
$P_{2,0}^{\mathrm{s}}$
$P_{2,1}^{\mathrm{s}}$
$P_{3,0}^{\mathrm{s}}$
$P_{3,1}^{\mathrm{s}}$
b
Noncontextual Models
0.0
0.2
0.4
0.6
0.8
1.0
A
0.996
0.998
1.000

Part IV

Direct cryptographic applications of contextuality?

Suggestion

A prepare-and-measure key distribution scheme which assumes only that Bob's measurements are tomographically complete for Alice's preparations (+ usual secure labs).

Toy analysis

Alice has four preparations, Bob has two binary measurements.

Toy analysis

Alice has four preparations, Bob has two binary measurements.
Alice and Bob measure $p(k|\mathcal{P}_i, \mathcal{M}_j)$.

Toy analysis

Alice has four preparations, Bob has two binary measurements.
Alice and Bob measure $p(k|\mathcal{P}_i, \mathcal{M}_j)$.
Consider an extra variable e, with

$$p(k, e|\mathcal{P}_i, \mathcal{M}_j) = p(e|\mathcal{P}_i)p(k|\mathcal{P}_i, e, \mathcal{M}_j)$$

Toy analysis

Alice has four preparations, Bob has two binary measurements.
Alice and Bob measure $p(k|\mathcal{P}_i, \mathcal{M}_j)$.
Consider an extra variable e, with

$$\begin{aligned} p(k, e|\mathcal{P}_i, \mathcal{M}_j) &= p(e|\mathcal{P}_i)p(k|\mathcal{P}_i, e, \mathcal{M}_j) \\ &= f_{k,e,j}\left(\{p(k'|\mathcal{P}_i, \mathcal{M}_{j'})\}_{k',j'}\right) \end{aligned}$$

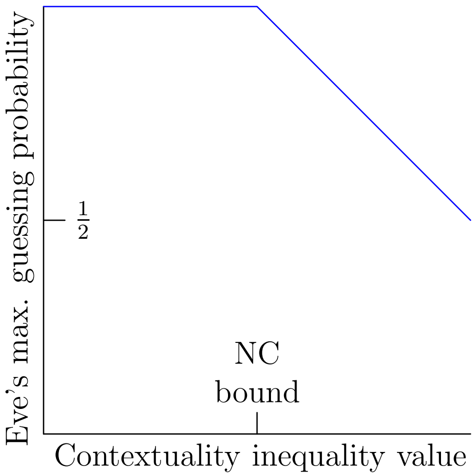
Toy analysis

Alice has four preparations, Bob has two binary measurements.
Alice and Bob measure $p(k|\mathcal{P}_i, \mathcal{M}_j)$.
Consider an extra variable e, with

$$\begin{aligned} p(k, e|\mathcal{P}_i, \mathcal{M}_j) &= p(e|\mathcal{P}_i)p(k|\mathcal{P}_i, e, \mathcal{M}_j) \\ &= f_{k,e,j}\left(\{p(k'|\mathcal{P}_i, \mathcal{M}_{j'})\}_{k',j'}\right) \end{aligned}$$

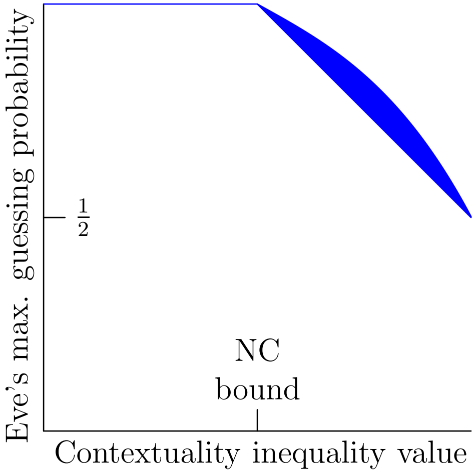
Maximize $\frac{p(e=0|\mathcal{P}_0)+p(e=1|\mathcal{P}_1)}{2}$

Results: simple case



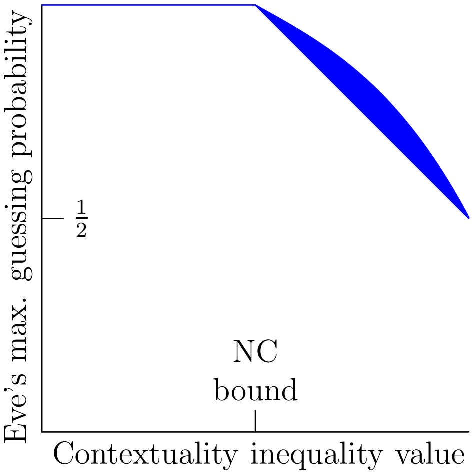
Contextuality inequality: arXiv:1506.04178

Results: general case



Contextuality inequality: arXiv:1506.04178

Results: general case



$$p(k|\mathcal{P}_i, \mathcal{M}_j) = \delta_{kb_i(j)}$$

Conclusions

- Provided one has a tomographically complete set of procedures, noncontextuality is robust both to failures of exact operational equivalence and to non-projective measurements
- Conjecture: key distribution can be secured by tomographic completeness
- However: better justifications for tomographic completeness are needed!

Main reference: arXiv:1505.06244