Testing randomness with photons by direct characterization of optical t-designs

Jonathan C. F. Matthews, Rebecca Whittaker, Jeremy L. O'Brien, and Peter S. Turner

Phys. Rev. A **91**, 020301 — Published 17 February 2015

DOI: 10.1103/PhysRevA.91.020301

Testing randomness with photons by direct characterisation of optical $t-$designs

Jonathan C. F. Matthews,[1, *] Rebecca Whittaker,[1] Jeremy L. O'Brien,[1] and Peter S. Turner[‡, 2, †]

[1] *Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering,*
University of Bristol, Merchant Venturers Building, Woodland Road, Bristol BS8 1UB, UK.
[2] *Department of Physics, Graduate School of Science,*
University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan 113-0033[‡]

Generating and characterising randomness is fundamentally important in both classical and quantum information science. Here we report the experimental demonstration of ensembles of pseudorandom optical processes comprising what are known as t-designs. We show that in practical scenarios, certain finite ensembles of two-mode transformations – 1- and 2-designs – are indistinguishable from truly random operations for 1- and 2-photon quantum interference, but they fail to mimic randomness for 2- and 3-photon cases, respectively. We make use of the fact that t-photon behaviour is governed by degree-$2t$ polynomials, (in the parameters of the optical process), to experimentally verify the ensembles' behaviour for *complete* bases of polynomials, ensuring that average outputs will be uniform for arbitrary configurations. It is in this sense that a t-design is deemed to be a potentially useful pseudorandom resource.

Introduction – Randomness is a workhorse in science and technology, from simulating complex systems and modelling error to probabilistic computation and information security. In quantum mechanics, randomness is a fundamental feature, but additional (classical) randomness can be a powerful resource when purposely introduced into quantum protocols; examples include quantum communication [1], quantum algorithms [2], quantum data hiding [3], benchmarking unknown quantum processes [4–8], and verifying the boson sampling conjecture [9]. However, truly random quantum operations are inefficiently realisable both in principle and in practice. Here we report the realisation and complete characterisation of *pseudorandom* photonic quantum operator ensembles: so-called *t-designs* that simulate statistical properties of truly random operators using fewer resources [10, 11]. We make use of the fact that t-photon behaviour is governed by degree-$2t$ polynomials, (in the optical process parameters), to perform complete experimental verification of the ensembles' behaviour. We realise a 1-design and a 2-design, and show that 1- and 2-photon quantum interference [12, 13] is sufficient for their complete verification. Furthermore, we show that 2- and 3-photon interference, respectively, can be used to test the limits of their pseudorandom properties. We apply these ideas to distinguish, with a fixed measurement setting, pseudorandom 1-design polarisation rotations from Haar random unitaries in a situation where process tomography using single photon states would fail.

Unitary processes transform one pure quantum state to another. Realising fair and unbiased random unitary operations requires sampling uniformly from a continuously infinite group. This group is equipped with a unique invariant (Haar) measure, which defines how one samples uniformly, without bias, over the whole set. However, "true" randomness is inefficiently realisable in practice, due to poor scaling of the number of random parameters with the size of the system. Fortunately, sampling uniformly from a restricted subensemble of unitary operators can be done efficiently and still exhibits some of the desired statistical properties of truly random processes. Such pseudorandom operations are therefore sought after for applications in quantum protocols. Randomly sampled unitaries have been implemented experimentally, for example in NMR [4, 5], trapped ion [7], solid state [8] and photonic [14] qubits.

This notion of pseudorandomness is captured well by *unitary t-designs*. These are subensembles of quantum operations that, given t copies of a system, are statistically indistinguishable from a uniformly distributed superensemble. Equivalently, they are subensembles that have the same t-th order moments as the uniform Haar ensemble, and thus they can be used to simulate statistical properties of truly random quantum operations with fewer resources. These statistical moments are given by polynomials in the parameters of the quantum operators in question, (see below). The work presented here is the first to directly characterise such pseudorandom operators experimentally.

Optical t-designs – Here we are concerned with the superensemble of all unitary polarisation rotations of an optical channel. Ignoring global phase, these are parameterised by real variables $\{x_1, y_1, x_2, y_2\}$ with the constraint $x_1^2 + y_1^2 + x_2^2 + y_2^2 = 1$, and expressed as

$$U = \begin{pmatrix} x_1 + iy_1 & x_2 + iy_2 \\ -x_2 + iy_2 & x_1 - iy_1 \end{pmatrix}. \tag{1}$$

Probability distributions that govern the outcomes of any multiphoton interference experiment are polynomials in these variables, whose degree is dictated by the number of photons. In general, t-photon interference is modelled by a degree-$2t$ polynomial in the matrix elements of the

[‡] Now at the School of Physics, H. H. Wills Physics Laboratory, Tyndall Avenue, University of Bristol, Bristol BS8 1TL, UK.
[*] Electronic address: `jonathan.matthews@bristol.ac.uk`
[†] Electronic address: `peter.turner@bristol.ac.uk`

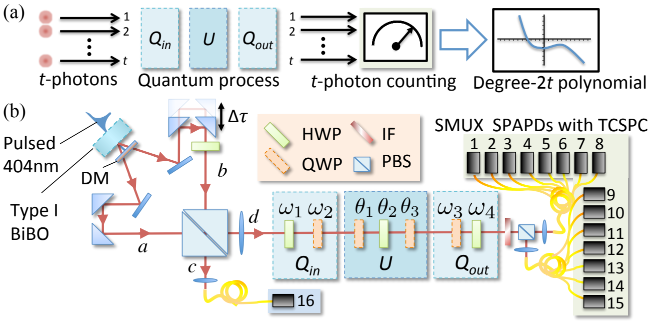

FIG. 1: (a) t-photon interference is described by degree-$2t$ polynomials. (b) Our setup samples complete sets of independent degree-2 [degree-4] polynomials in the matrix elements of U using interference of 1-photon [2-photon] states, generated from spontaneous parametric downconversion (SPDC) in type-1 BiBO. Polarized photon pairs generated in paths a and b are combined onto d in the photon-number state $|1\rangle_H |1\rangle_V$, using a half-wave plate (HWP) and a polarising beam splitter (PBS). Degree-6 polynomials were sampled with the 3-photon state $|2\rangle_H |1\rangle_V$ in path d, observed by post-selecting from the four-photon term of pulsed SPDC state: 3-photons detected across single photon avalanche diodes (SPADs) 1 - 15 and one photon heralded at SPAPD 16 (see Supplemental Material for further details). The quantum process $T = Q_{\rm out} U Q_{\rm in}$ was implemented using wave plates (QWP, HWP, dashed boxes). Photon-number-resolving detection [15] uses spatially multiplexed (SMUX) SPADs (1-15), used in conjunction with a commercial 16-channel time-correlated single photon counting system (TCSPC).

unitary process [16] (Fig. 1(a)). For example, the transition probability of one photon from input 2 to output 2 is the degree-2 polynomial $|U_{2,2}|^2 = x_1^2 + y_1^2$, (note that this exactly agrees with how the intensity of classically modelled light is distributed as it passes through U). Degree-4 polynomials describe two-photon non-classical interference, including the probability to detect one photon in each output of U in a Hong-Ou-Mandel experiment [12], given by [13] $|U_{1,1}U_{2,2} + U_{1,2}U_{2,1}|^2$.

A unitary t-design [11] is defined in terms of such polynomials. Explicitly, a finite set $\mathfrak{D}_t$ containing K unitary operators, viewed as an ensemble with uniform distribution $1/K$, is defined to be a t-design if *every* degree-$2t$ polynomial [25] in the matrix elements of U, $f_{2t}(U)$, has the same average over $\mathfrak{D}_t$ as it does when averaged over the uniform ensemble of *all* unitaries;

$$\mathbb{E}_{\mathfrak{D}_t}[f_{2t}] = \sum_{U \in \mathfrak{D}_t} \frac{1}{K} f_{2t}(U) = \int \mathrm{d}U \; f_{2t}\,(U) = \mathbb{E}_{\rm Haar}[f_{2t}]. \quad (2)$$

Uniformity in the continuous case is defined by the normalised unitary Haar measure dU, and there are methods for computing the integral over the unitary group, (e.g. Ref. 19). Note that a t-design is by definition also a $(t-1)$-design, hence experiments with t or fewer photons sampled over a t-design are statistically indistinguishable from the same experiments with operations sampled from the Haar distribution. Multiphoton interference, being governed by such polynomials, can therefore be used to verify the realisation of a t-design, and ($>t$)-photon interference can also be used to test pseudorandomness as an alternative to standard process tomography.

The unitary operators we use to realise a 1-design are drawn from the uniformly distributed Pauli ensemble [26]

$$\mathfrak{D}_1 = \{I, iX, -iY, iZ\}\,. \quad (3)$$

Evidence that $\mathfrak{D}_1$ is a 1-design follows from the fact that single photons sequentially input into mode 1 will be distributed equally between output 1 (due to I and Z) and output 2 (due to X and Y), which agrees with the full Haar distributed random ensemble of SU(2) rotations: $\mathbb{E}_{\rm Haar}[|U_{1,1}|^2] = \mathbb{E}_{\rm Haar}[|U_{1,2}|^2] = 1/2$. A proof that $\mathfrak{D}_1$ is a 1-design can be obtained by showing the equality in Eq. (2) holds for each element of a complete basis of independent, degree-2 monomials in the real variables x_1, y_1, x_2, y_2; assuming unitarity there are nine, we choose:

$$f_2 \in \left\{x_1^2, x_1x_2, x_2^2, x_1y_1, x_1y_2, x_2y_1, x_2y_2, y_1^2, y_1y_2\right\}. \quad (4)$$

It is intuitive from a quantum optics perspective to see that $\mathfrak{D}_1$ is not a 2-design. Consider a Hong-Ou-Mandel experiment where we estimate the probability for two indistinguishable photons input into ports 1 and 2 to anti-bunch at the two outputs [12]. When U corresponds to a 50:50 beamsplitter then there is ideally zero probability to detect one photon at each output. Therefore, when sampling over the entire Haar ensemble, the average probability for the photons to anti-bunch must be strictly less than 1. Averaging over $\mathfrak{D}_1$, however, will always yield an anti-bunching probability of exactly 1, hence Eq. (2) will not hold for all degree-4 polynomials.

The uniform ensemble of twelve operators listed in Table I *is* a 2-design, $\mathfrak{D}_2$. This is confirmed by showing Eq. (2) is satisfied with respect to the complete basis of (again, assuming unitarity) 25 degree-4 monomials:

$$\begin{aligned} f_4 \in \{&x_1^4, x_1^3x_2, x_1^2x_2^2, x_1x_2^3, x_2^4, x_1^3y_1, x_1^2x_2y_1, x_1x_2^2y_1, x_2^3y_1, \\ &x_1^3y_2, x_1^2x_2y_2, x_1x_2^2y_2, x_2^3y_2, x_1^2y_1^2, x_1x_2y_1^2, x_2^2y_1^2, x_1^2y_1y_2, \\ &x_1x_2y_1y_2, x_2^2y_1y_2, x_1y_1^3, x_1y_1^2y_2, x_2y_1^3, x_2y_1^2y_2, y_1^4, y_1^3y_2\}. \end{aligned} \quad (5)$$

Experiment— We implement each element of $\mathfrak{D}_2$ (and $\mathfrak{D}_1$) using a combination of two quarter-wave plates and one half-wave plate, as shown in the box labeled U in Fig. 1 (b), with the settings θ_i given in Table I.

To verify experimentally that an ensemble $\mathfrak{D}_t$ of unitaries is a t-design, we must have access to a complete basis of polynomials; this requires some added control over the optical transformation. We achieve this by adding the reconfigurable polarisation transformations ($Q_{\rm in}, Q_{\rm out}$), yielding the total unitary $T := Q_{\rm out} U Q_{\rm in}$, shown in Fig. 1. For each choice of configuration, the transition probability from a fixed input to a fixed output is a polynomial in the elements of U; thus we can now choose polynomials. The wave plate settings for ($Q_{\rm in}, Q_{\rm out}$) corresponding to our choice are given in Table II, labelled according to Fig. 1(b). We find these settings give complete bases of linearly independent [27] degree-2 and degree-4 polynomials as follows; nine 1-photon output probabilities corresponding to $|T_{1,1}|^2$, which we label $p_1, ..., p_9$

$U \in \mathfrak{D}_2$	θ_1	θ_2	θ_3
I	0	90	0
iX	0	-45	0
$-iY$	45	90	-45
iZ	-45	90	-45
$(I+iX-iY+iZ)/2$	0	90	-45
$(I+iX+iY+iZ)/2$	-45	90	0
$(I-iX-iY+iZ)/2$	45	90	0
$(I-iX+iY+iZ)/2$	0	90	45
$(I+iX-iY-iZ)/2$	45	-45	0
$(I+iX+iY-iZ)/2$	0	-45	45
$(I-iX-iY-iZ)/2$	0	45	-45
$(I-iX+iY-iZ)/2$	-45	45	0

TABLE I: The wave plate settings for θ_i in degrees, as labeled in Fig. 1.(b), to realise the elements of $\mathfrak{D}_2 \supset \mathfrak{D}_1$. We adopt the convention that rotation angles are from the vertical.

p_i	ω_1	ω_2	ω_3	ω_4	p_i	ω_1	ω_2	ω_3	ω_4
p_1	0	0	0	0	p_6	0	22.5	0	22.5
p_2	0	0	0	22.5	p_7	0	22.5	22.5	0
p_3	0	0	0	45	p_8	0	45	0	0
p_4	0	0	22.5	0	p_9	0	45	0	22.5
p_5	0	22.5	0	0					

q_i	ω_1	ω_2	ω_3	ω_4	q_i	ω_1	ω_2	ω_3	ω_4
q_1	0	0	0	0	q_{14}	0	45	0	60
q_2	0	0	0	22.5	q_{15}	0	45	22.5	0
q_3	0	0	0	60	q_{16}	0	45	22.5	22.5
q_4	0	0	22.5	0	q_{17}	0	60	0	0
q_5	0	0	22.5	22.5	q_{18}	0	60	0	22.5
q_6	0	0	45	22.5	q_{19}	0	60	0	60
q_7	0	22.5	0	0	q_{20}	0	60	22.5	0
q_8	0	22.5	0	22.5	q_{21}	0	60	22.5	22.5
q_9	0	22.5	0	60	q_{22}	0	120	0	0
q_{10}	0	22.5	22.5	0	q_{23}	0	120	0	22.5
q_{11}	0	22.5	22.5	22.5	q_{24}	0	120	0	60
q_{12}	0	45	0	0	q_{25}	0	120	22.5	0
q_{13}	0	45	0	22.5					

TABLE II: Wave plate settings ω_i in degrees for Q_{in}, Q_{out}, as labeled in Fig. 1.(b), for accessing polynomials p_i (1-photon experiments) and q_i (2-photon experiments).

(*e.g.* $p_1 = x_1^2 + {y_1}^2$), and a set of 25 2-photon probabilities $|T_{1,1}T_{2,2} + T_{1,2}T_{2,1}|^2$, which we label $q_1, ..., q_{25}$ (*e.g.* $q_1 = x_1^4 - 2x_1^2x_2^2 + 2x_1^2y_1^2 + x_2^4 - 2x_2^2y_1^2 + y_1^4$). We then average each probability over $U \in \mathfrak{D}_t$, implemented as given in Table I, and thus arrive at an estimate for the LHS of Eq. (2) that we can use to verify uniformity.

Results — Figure 2 shows normalised 1-photon intensities $|T_{1,1}|^2$ extracted from the experiment, taken for $p_1, .., p_9$ and averaged uniformly over the ensembles $\mathfrak{D}_1$ (Fig. 2 (a)) and $\mathfrak{D}_2$ (Fig. 2 (b)). Both agree with the uniform Haar average over all unitaries. Since $p_1, .., p_9$ are a complete basis, this agreement directly verifies the two ensembles $\mathfrak{D}_1$ and $\mathfrak{D}_2$ are both at least unitary 1-designs.

The difference in the behaviour of $\mathfrak{D}_1$ and $\mathfrak{D}_2$ is clear when observing 2-photon interference. Fig. 3 shows expected and measured 2-photon correlations $|T_{1,1}T_{2,2} + T_{1,2}T_{2,1}|^2$ taken for $q_1, .., q_{25}$ and averaged uniformly over the ensembles $\mathfrak{D}_1$ (Fig. 3 (a)) and $\mathfrak{D}_2$ (Fig. 3 (b)). The average of degree-4 polynomials over $\mathfrak{D}_1$ shows behaviour clearly distinct from the uniform behaviour that would be observed from averaging over the Haar measure (black dashed lines). Together with the results of Fig. 2 (a), this agreement directly verifies the ensemble $\mathfrak{D}_1$ is a 1-design only. In contrast, the uniformity of the degree-4 polynomials averaged over $\mathfrak{D}_2$ (Fig. 2 (b)) agrees closely with the average over the Haar measure. Since $q_1, ..., q_{25}$ is a complete set of degree-4 polynomials, this verifies the ensemble $\mathfrak{D}_2$ is at least a 2-design. For completeness, Fig. 3 (c) shows 2-photon interference statistics averaged over a set of 12 matrices chosen from the Haar distribution [20]. The data illustrate that in general an ensemble of twelve operations—the size of $\mathfrak{D}_2$—is not sufficient to simulate the Haar average, though of course a larger en-

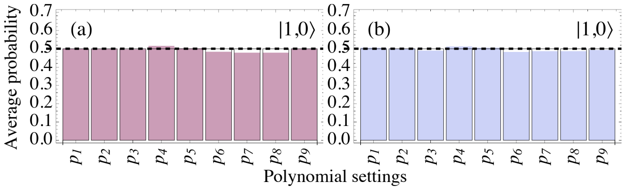

FIG. 2: Polynomials $p_1, ...p_9$ extracted from the measured normalised single photon intensity $|T_{1,1}|^2$, averaged over settings corresponding to (a) $\mathfrak{D}_1$, and (b) $\mathfrak{D}_2$. Measured distributions (solid colour) are plotted with ideal theoretical values (empty boxes). Dashed lines represents the ideal Haar value $P_H = 1/2$, which is always uniform for normalised probability distributions.

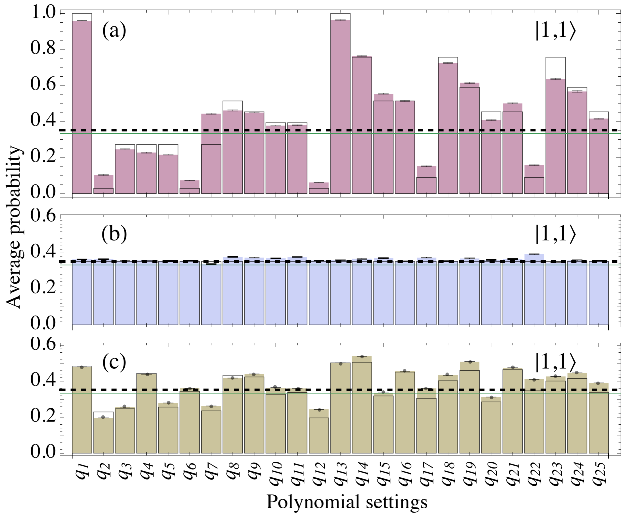

FIG. 3: Polynomials $q_1, ..., q_{25}$ extracted from experiment by measuring the 2-photon correlation $|T_{1,1}T_{2,2} + T_{1,2}T_{2,1}|^2$ and averaging over settings that correspond to realising (a) $\mathfrak{D}_1$, (b) $\mathfrak{D}_2$, and for comparison (c) twelve unitary operators chosen randomly from the Haar distribution that do not form a 2-design. Photon distinguishability alters the realised polynomials from their ideal values and the average they would converge to when sampling U over a Haar distribution (green line). This is characterised in the experiment and the ideal theoretical polynomials (empty boxes) and the Haar average (dashed line) are corrected accordingly (see Supplemental Material for details). The average statistical fidelity, $\sum_i \sqrt{p_i q_i}$, between the probability distributions extracted from our experiment and the ideal distributions is $99.26 \pm 0.02\%$ for the 600 2-photon experiments used to generate these plots.

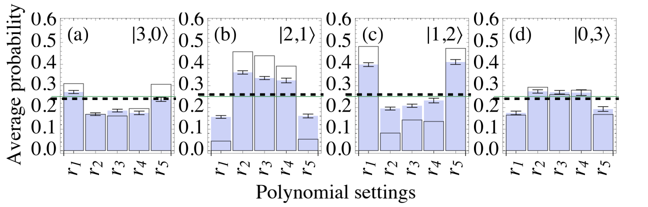

FIG. 4: Detection outcomes for 3-photon polynomials r_i, averaged over $\mathfrak{D}_2$. Solid colour represents measured data, empty boxes represent theory and error bars are computed from assuming Poisson-distributed detection noise. Haar averages for perfect interference and characterised photon-distinguishability are marked by the black dashed and green lines respectively. The average statistical fidelity between measured probability distributions and theory is $97.55 \pm 0.03\%$ for the 72 3-photon experiments.

semble eventually will (see Refs 21, 22 for convergence results). As t increases, it will be harder to distinguish between t- and $(t+1)$-designs due to experimental noise.

To complete the characterisation of $\mathfrak{D}_2$, we use 3-photon interference for a set of five arbitrarily chosen degree-6 polynomial settings (labeled $r_1, ..., r_5$, with wave plate settings given in Table III). The data are shown in Fig. 4, verifying that $\mathfrak{D}_2$ is not a 3-design due to the existence of polynomials whose average over $\mathfrak{D}_2$ differs from the Haar value. Note that a single degree-6 polynomial that deviates from the Haar average is sufficient to demonstrate failure to simulate the Haar distribution.

p_i	ω_1	ω_2	ω_3	ω_4	p_i	ω_1	ω_2	ω_3	ω_4
r_1	94.0	117.3	64.9	24.5	r_4	179.7	11.36	24.6	108.1
r_2	129.5	67.1	118.3	6.8	r_5	1.9	114.0	162.5	160.7
r_3	112.8	67.9	159.2	3.6					

TABLE III: Wave plate settings ω_i in degrees to access a selection degree-6 polynomials using 3-photons.

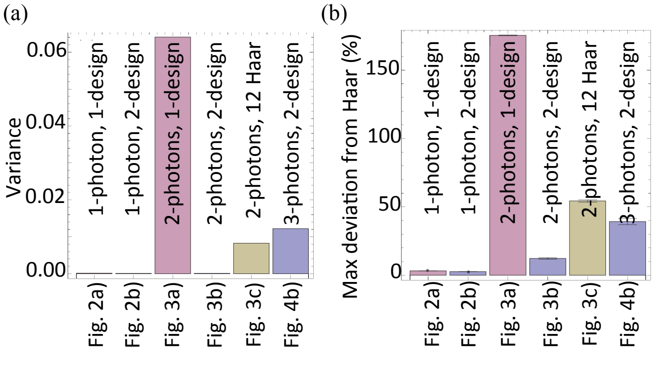

FIG. 5: Uniformity of each data set, plotted in terms of (a) the variance over the set of polynomials measured and (b) the maximum deviation of the average probability, as a percentage, from the expected Haar average (black dashed line in Fig. 2 and green solid lines in Figs. 3 and 4).

Analysis of uniformity – How accurately the finite ensembles we realise mimic Haar distributed unitary matrices can be quantified by the uniformity of the average probabilities over the different polynomial settings, and how much they deviate from the expected Haar average in each case. We quantify the uniformity of the ensemble behaviour in Fig. 5; note that while theory predicts that t-photon interference over a t-design should yield perfectly uniform results, experimental imperfections in realising design elements can give rise to non-uniformity. Figure 5 indicates that variance in particular is an excellent discriminator for t-designs.

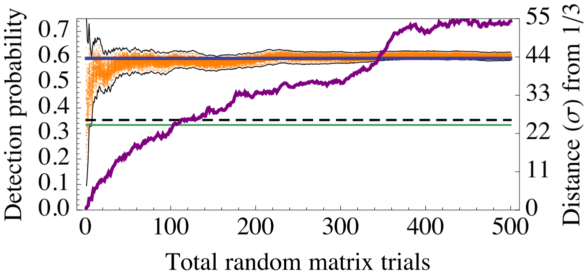

FIG. 6: *Left-hand axis:* Running average of $P_{est} = |T_{1,1}T_{2,2} + T_{1,2}T_{2,1}|^2$ estimated from each of sixty-four independent 2-photon experiments (overlaid orange points) as U implements uniformly at random elements of $\mathfrak{D}_1$ for polynomial q_{19}. The blue line marks the value that P_{set} should ideally converge to, taking into account characterised indistinguishability of photon pairs (see Supplemental Material). Green and black dashed lines mark the values that P_{est} would converge to when sampling uniformly from the Haar measure, for perfect and characterised indistinguishability respectively. *Right-hand axis, purple line:* The number of standard deviations that P_{est} differs from the Haar average $P_H = 1/3$, quantifying confidence of directly discriminating a non-Haar ensemble.

Example application – If a random optical channel is fluctuating slowly, then the ensemble could be broken down into its constituent elements and each interrogated by full process tomography [23], enabling x_1, y_1, x_2, y_2 to be reliably estimated and condition Eq. 2 tested mathematically. When probing individual elements of an ensemble is limited, it may be convenient to use multi-photon states with a fixed measurement to directly distinguish an ensemble from the Haar ensemble. Fig. 6 shows the real-time failure of a photonic 1-design to behave Haar-randomly in the low photon rate regime. The wave plate configurations U were set to realise uniformly at random one of the four $\mathfrak{D}_1$ operations, and Q_{in} and Q_{out} were fixed to realise the polynomial q_{19}. For each implementation of U, we estimate the probability distribution of each 2-photon detection outcome using $O(10)$ correlated detection events, which yields a noisy estimate of the distribution that is insufficient to perform reliable process tomography; this could be performed with on average a single photon-pair for each U by further attenuation. As we increase the number of samples of $\mathfrak{D}_1$ from 1 to 500, we compute a running average for the estimate of $P_{\text{est}} = |T_{1,1}T_{2,2} + T_{1,2}T_{2,1}|^2$ which converges to a value of 0.603 ± 0.001. For characterised photon indistinguishability, P_{est} should converge to 0.594 (blue line). Confidence that we are not sampling U according to the Haar measure is quantified by the number of standard deviations P_{est} is from $P_{\text{H}} = 1/3$—for example, for 11 trials (~ 220

photon pairs) is more than 6 standard deviations.

Conclusion – We have realised unitary 1- and 2-designs in two dimensions, using multiphoton interference for a complete verification of their pseudorandom properties. To do so, we have made use of the fact that multiphoton transition probabilities are polynomials in the matrix elements of optical unitaries. In general, $(t+1)$-photon interference can be used to distinguish a t-design from a truly random ensemble of unitary operations. Although this can be mimicked with a reduced visibility of interference features using intensity correlation measurements of several input light fields [17], reaching the same visibility requires an overhead in measurement and data analysis [18],[28]. Furthermore, we have demonstrated a scenario where standard process tomography would be incapable of inferring the 'degree' of randomness (as given by a value of t). Interestingly, it has been suggested that such ensembles will likely be required to demonstrate conjectured extra-classical capabilities of linear quantum optics [24].

[1] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, Proc. R. Soc. A **465**, 2537–2563 (2009).

[2] J. Radhakrishnan, M. Rötteler, and P. Sen, Algorithmica **55**, 490–516 (2009).

[3] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Commun. Math. Phys. **250**, 371–391 (2004).

[4] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory, Science **302**, 2098–2100 (2003).

[5] J. Emerson, M. Silva, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D. G. Cory, and R. Laflamme, Science **317**, 1893–1896 (2007).

[6] J. M. Epstein, A. W. Cross, E. Magesan, and J. M. Gambetta, Phys. Rev. A **89**, 062321 (2014).

[7] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, Phys. Rev. A **77**, 012307 (2008).

[8] J. M. Chow, J. M. Gambetta, L. Tornberg, J. Koch, L. S. Bishop, A. A. Houck, B. R. Johnson, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, Phys. Rev. Lett. **102**, 090502 (2009).

[9] S. Aaronson and A. Arkhipov, Proceedings of the 43rd annual ACM symposium on Theory of computing pp. 333–342 (2011).

[10] D. Gross, K. Audenaert, and J. Eisert, J. Math. Phys. **48**, 052104 (2007).

[11] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Phys. Rev. A **80**, 012304 (2012).

[12] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).

[13] K. Mattle, M. Michler, H. Weinfurter, A. Zeilinger, and M. Zukowski, Appl. Phys. B **60**, S111 (1995).

[14] K. Banaszek, R. Demkowicz-Dobrzanski, M. Karpinski, P. Migdal, and C. Radzewicz, Opt. Commun. **283**, 713–718 ((2010)).

[15] D. Achilles, C. Silberhorn, C. Silwa, K. Banaszek, I. A. Walmsley, M. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, Journal Mod. Opt. **51**, 1499–1515 (2004).

[16] Y. L. Lim and A. Beige, New J. Phys. **7**, 155 (2005).

[17] Y. Bromberg, Y. Lahini, R. Morandotti, and Y. Silberberg, Phys. Rev. Lett. **102**, 253904 (2009).

[18] R. Keil, F. Dreisow, M. Heinrich, A. Tünnermann, S. Nolte, and A. Szameit, Phys. Rev. A **83**, 013808 (2011).

[19] B. Collins and P. Sniady, Commun. Math. Phys. **264**, 773–795 (2006).

[20] F. Mezzadri, Notices of the AMS **54**, 592–604 (2007).

[21] A. W. Harrow and R. A. Low, Commun. Math. Phys. **291**, 257 (2009).

[22] F. G. S. L. Brandao, A. W. Harrow, and M. Horodecki, arXiv:1208.0692 (2012).

[23] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[24] C. Gogolin, M. Kliesch, L. Aolita, and J. Eisert, arXiv:1306.3995 (2013).

[25] Elsewhere t-designs have been defined such that a distinction is made between the degrees of conjugate variables, but here we use only the real variables $\{x_1, y_1, x_2, y_2\}$.

[26] The phases were chosen to give a representation of the unit quaternions $\mathbf{1} \leftrightarrow I$, $\mathbf{i} \leftrightarrow iX$, $\mathbf{j} \leftrightarrow -iY$ and $\mathbf{k} \leftrightarrow iZ$.

[27] Linear independence of the polynomials is confirmed by checking that the Gram matrix, defined here as the matrix of coefficients of a set of polynomials in the monomial basis, is full rank (9 for $t=1$, 25 for $t=2$).

[28] Ref. 18 uses three configurations to reconstruct the expansion of a two-photon quantum walk correlation function. Simulation of n-photon interference in this manner requires measurement and data analysis that grows with the $n!$ terms in the n-photon correlation function.

Acknowledgments

We thank E. Hemsley, P. J. Shadbolt, X.-Q. Zhou, S. Bartlett, S. Vinjanampathy, H. Cable and J. Eisert for helpful discussions, and especially T. Rudolph for the premise and advice. The authors are grateful for financial support from the US Army Research Office, EPSRC, ERC, NSQI. J.C.F.M. and P.S.T. are grateful for financial support from the EPSRC BGER. J.C.F.M. is supported by a Leverhulme Trust Early Career Fellowship. J.L.O.B. acknowledges a Royal Society Wolfson Merit Award and a Royal Academy of Engineering Chair in Emerging Technologies.