Photonic Quantum Information Processing
OPTI 647: Lecture 1

Saikat Guha

August 27, 2019

Associate Professor
College of Optical Sciences
Meinel 523

Logistical information

- Course instructor: Saikat Guha, saikat@optics.arizona.edu, OSC 523, (520) 621-7595
- Course assistant: Brianna Moreno, bmoreno@optics.arizona.edu, OSC 501, (520) 621-4842
- Lectures 8 am – 9:15 am Tuesdays and Thursdays, OSC 307
- Office hours 11 am – noon, Wednesdays, 11-noon?
- Problem sets – problems assigned during lectures, due by Monday noon, submit to Brianna Moreno at OSC 501
  - First problem set will be due Tuesday, September 3
- Last two lectures: 15-minute student presentations on one “advanced” homework problem(s) of your own choice
- Grading: problem sets (70%), presentation (30%): A/B/C/D/F

Pre-requisites

- Basic quantum mechanics
  - unless arranged with instructor
- Mathematical preparation
  - Complex numbers
  - Basic linear algebra (matrices, eigenvalues, etc.)
  - Probability: random variables and random processes
  - Calculus
  - Fourier transforms (basic)
- Software
  - MATLAB (or, equivalent)

Some related courses

- OPTI 595B “Information in a Photon”, Prof. Saikat Guha
  - Focus on quantum information theory and quantum estimation theory, applications to optical communications and sensing
- ECE 501B; “Quantum Information Processing and Quantum Error Correction”, Prof. Quntao Zhuang
  - Focus on quantum error correction, quantum computation and algorithms, entanglement, quantum sensing (this year)
- OPTI 646; “Introduction to Quantum Information and Computation”, Prof. Poul Jessen
  - Introductory quantum optics, quantum gates, circuits, algorithms, physical implementations (atomic/SC/ions)
- OPTI 570; “Quantum Mechanics”, Prof. Brian Anderson
  - Graduate level quantum mechanics, some quantum optics

Preamble

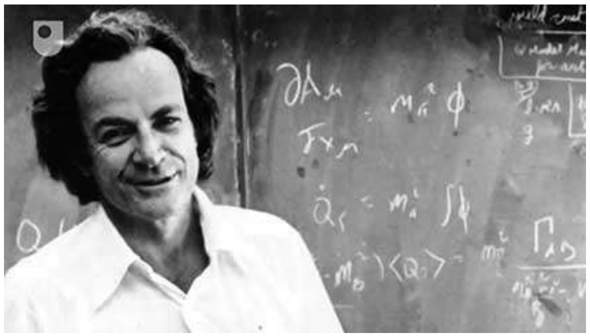
THE UNIVERSITY OF ARIZONA

- All forms of light, processing of light, and detection of light is fundamentally governed by quantum physics
  - Some forms of light, processing, and detection needs quantum theory to describe their behavior correctly. For some, semiclassical (shot-noise) theory suffices
- Quantum processing of information is more powerful
- Quantum information and estimation theories
  - Evaluating fundamental limits in optics based information processing (e.g., communication, sensing, imaging)
  - Optical detection *must* add noise
  - This noise degrades quality of information extraction
  - Information-bearing light may be manipulated in the optical domain. This can result in the *inevitable* detection noise to affect the information extraction efficiency favorably

Course outline

- Modal theory
- Mathematics of quantum optics: states, transformations, and measurements
- Spatio-temporal analysis of quantum non-linear optics: preparation of non-classical states of light
- “Quantifying” quantum information
- Photonic quantum information processing: application study

Quantum information processing



International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

SIAM J. COMPUT. © 1997 Society for Industrial and Applied Mathematics
Vol. 26, No. 5, pp. 1484–1509, October 1997 009

POLYNOMIAL-TIME ALGORITHMS FOR PRIME FACTORIZATION AND DISCRETE LOGARITHMS ON A QUANTUM COMPUTER*

PETER W. SHOR†

Evolution of physical systems is governed by quantum mechanical principles, which is hard to compute on a classical computer. Can we design physical systems as "computers" to mimic other physical systems of interest? E.g., simulating molecular systems for drug discovery

Qubit is the simplest quantum physical system. If we replaced every bit in our computers with qubits, it will be able to solve problems cannot be solved on our classical computer. E.g., Finding factors of a large number (current internet security relies on factoring being hard!)

Quantum computing

Factoring: $M = p \times q$

M =
109417386415705274218097073220403576120037329454492059909138421314763499842889347847179972578912673324976257528997818337970765372440271467435315933543338897

p = 102639592829741105772054196573991675900716567808038066803341933521790711307779

q = 106603488380168454820927220360012878679207958575989291522270608237193062808643

This was factored on August 22, 1999 in a span of six months, by a team led by Herman te Riele

The factorization was found using the **general number field sieve algorithm** and an estimated 4000 days worth of computational time on a 1GHz clock computer

Example: factor a 300-digit number

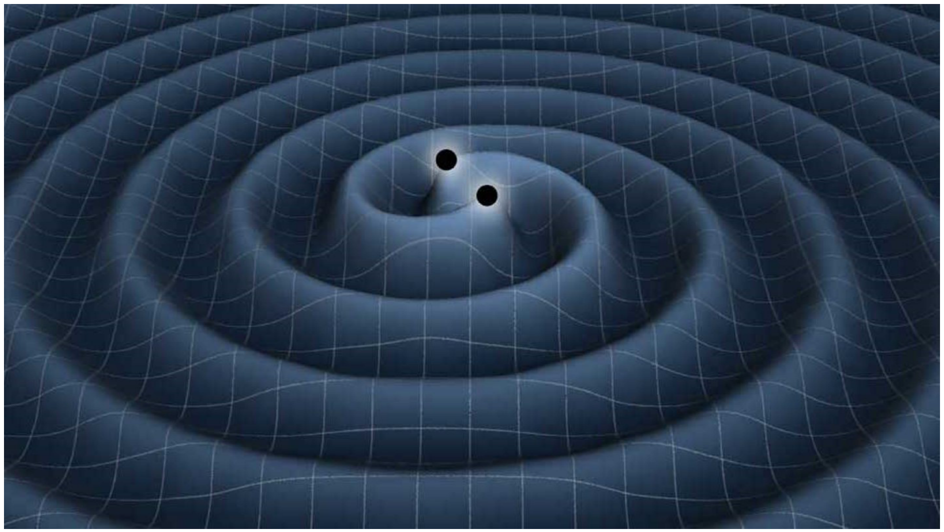
Best classical algorithm: 10^{24} steps	Shor's quantum algorithm: 10^{10} steps
On classical THz computer: 150,000 years	On quantum THz computer: <1 second

Shor's **quantum algorithm** can factor numbers very quickly

Difficulty of factorizing is the basis for modern cryptosystems used on the internet

LIGO: Laser Interferometer Gravitational-Wave Observatory

THE UNIVERSITY OF ARIZONA

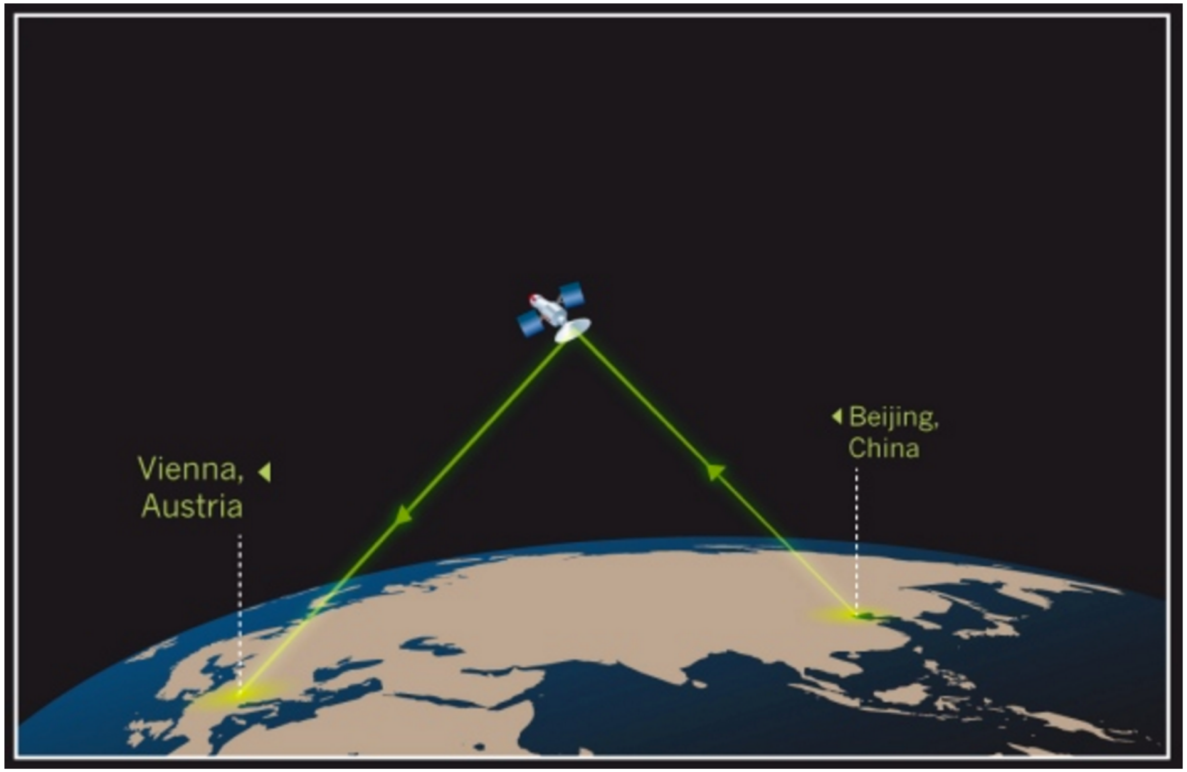


Quantum (squeezed) light can enhance sensitivity of estimating a small unknown phase modulation

$$\mathrm{MSE} \sim \frac{1}{N} \;\rightarrow\; \mathrm{MSE} \sim \frac{1}{N^2}$$

Quantum secured communications

- Un-decodable communications: Quantum *key distribution* (QKD)
- Un-detectable communications: Quantum secured *covert* communications



Quantum enhanced photonic information processing

THE UNIVERSITY OF ARIZONA

Communications

Higher capacity communications for deep space lasercom with quantum enabled receivers

Quantum networking: Communicating classical bits and quantum bits (qubits) reliably, generating shared entangled bits (ebits), Networked communications

Imaging and sensing

Active imaging and sensing: Quantum-enhanced ranging, metrology, velocimetry, vibrometry, atomic force microscopy, spectroscopy, reading

Passive imaging and sensing: Super-resolution passive imaging, hyperspectral imaging

Computing

Quantum computing

- Factoring, Discrete Log
- Search (e.g., on graphs)
- Simulations: chemistry, cond.-matter

Special purpose computing

- Quantum annealing
- Boson sampling
- Quantum receivers (comm, sensing)

Physics-based security

Secure communication

- Quantum key distribution (QKD)
- Covert communications and sensing

Secure multiparty (classical and quantum) computing

- Digital signatures
- Private-bid auctions
- Symmetric private information retrieval
- Blind quantum computing

Notion of an optical "mode"

Modes

- An optical mode is the "shape" of a confined EM field in space, time and polarization (the three independent degrees of freedom of the photon)
- Time & Frequency are the same degree of freedom (related by Fourier transform)

$$\phi_\nu(\boldsymbol{r},t);\ \boldsymbol{r} \in \mathcal{A}, t \in [0,T), \nu = 1,2$$

$$\int_{\mathcal{A}} \int_0^T \phi_\nu(\boldsymbol{r},t)\phi_\nu^*(\boldsymbol{r},t) d\boldsymbol{r} dt$$

$$= \int_{\mathcal{A}} \int_0^T |\phi_\nu(\boldsymbol{r},t)|^2 \, d\boldsymbol{r} dt = 1$$

We will take a mode to be normalized

Orthogonal modes

- Two modes $\phi_\nu(\boldsymbol{r}, t)$ and $\psi_\mu(\boldsymbol{r}, t)$ are **orthogonal** if,

$$\int_{\mathcal{A}} \int_0^T \phi_\nu(\boldsymbol{r}, t)\psi_\mu^*(\boldsymbol{r}, t) d\boldsymbol{r} dt = 0$$

  - If $\nu \neq \mu$, the two modes will be orthogonal regardless of their spatial and temporal shapes
  - When $\nu = \mu$, we will drop the polarization subscript
  - When we say two "temporal modes" $s_1(t)$ and $s_2(t)$ are orthogonal, we will implicitly assume the mode functions being referred to have the same spatial modes and polarization

Maximum number of orthogonal modes

- Consider temporal modes, $\phi_k(t), k = 1, \ldots K$
- …and their Fourier transforms,

$$\Phi_k(f) = \int \phi_k(t) e^{-2\pi j f t} dt$$

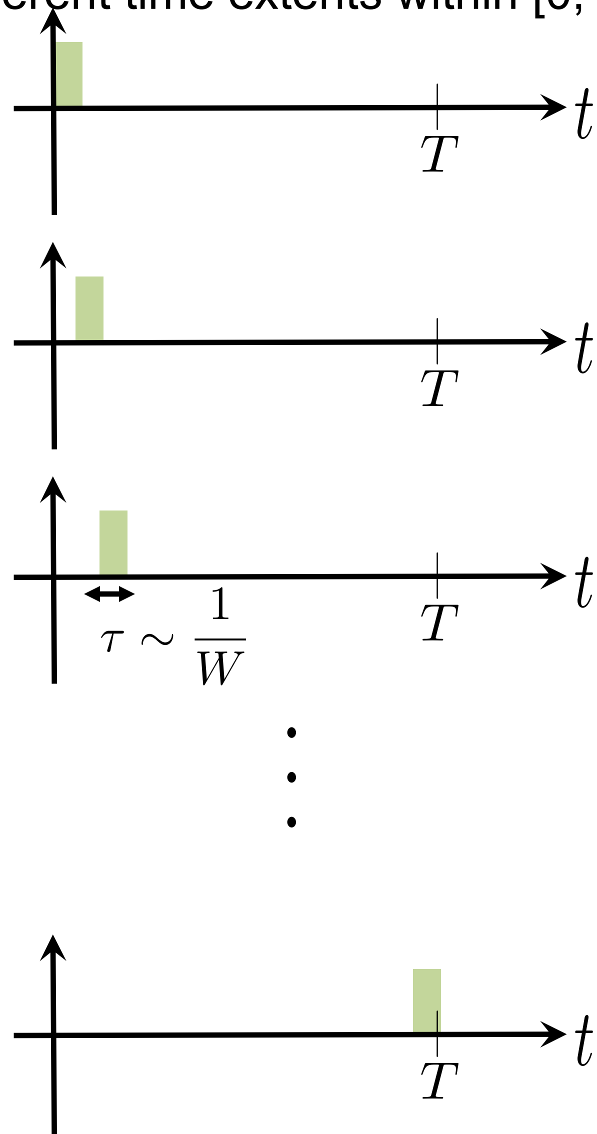
$$\phi_k(t) = \int \Phi_k(f) e^{2\pi j f t} df$$

- How many (K) orthogonal modes $\phi_k(t)$ can be "fit into" a time-bandwidth product of T x W? i.e.,
  - $\phi_k(t) = 0, t \notin [0, T)$, and $\Phi_k(f) = 0,\ f - f_0 > \left|\frac{W}{2}\right|$
  - While ensuring orthogonality: $\int_0^T \phi_k(t) \phi_l^*(t) dt = \delta_{kl}$
- Answer: $K \approx WT$, and these optimal mode functions are "Prolate Spheroidal" functions
- All of above holds for spatial modes as well

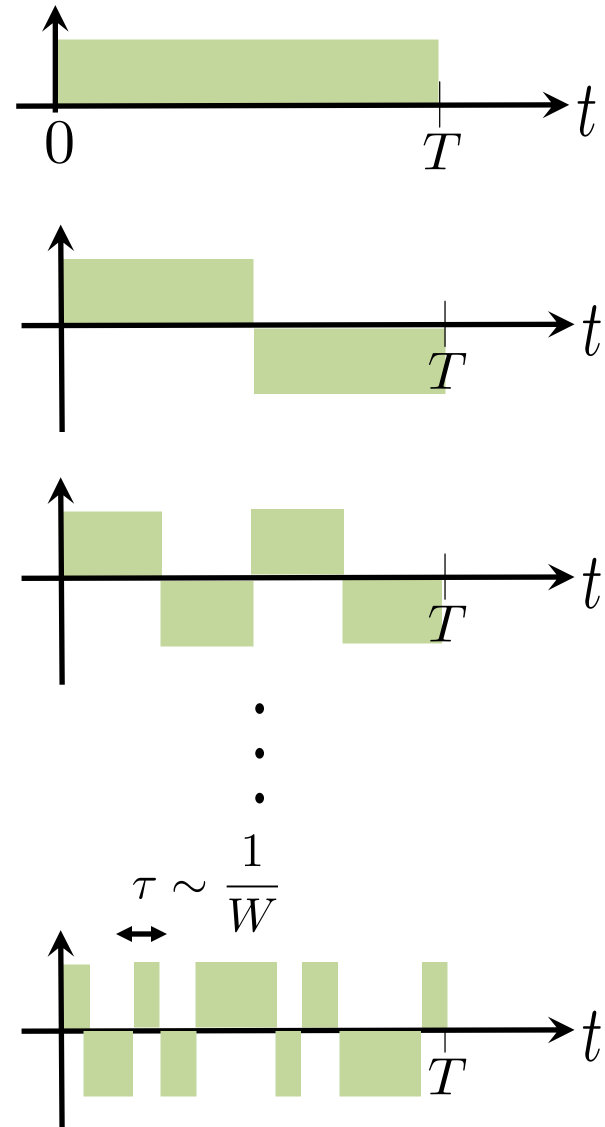
Slepian, D. Prolate spheroidal wave functions, Fourier analysis and uncertainty — IV: Extension to many dimensions; Generalized prolate spheroidal functions Bell Syst. Tech. J., vol. 43, pp. 3009-3057, Nov. 1964.

Some intuition: choices of WT modes

Each mode fills up the same BW, but different time extents within [0, T)



Each mode fills up the same time [0, T), but different freq extents within [-W/2, W/2]



Coherent state “of a mode”

- Consider a temporal mode: $\phi(t), t \in [0, T)$
- And a $\sqrt{\text{photons/sec}}$ unit field $E(t) = a\phi(t)e^{j2\pi f_0 t+\theta}$ of a temporal pulse
  – Take a to be real valued, WLOG
- The mean photon number in the pulse:

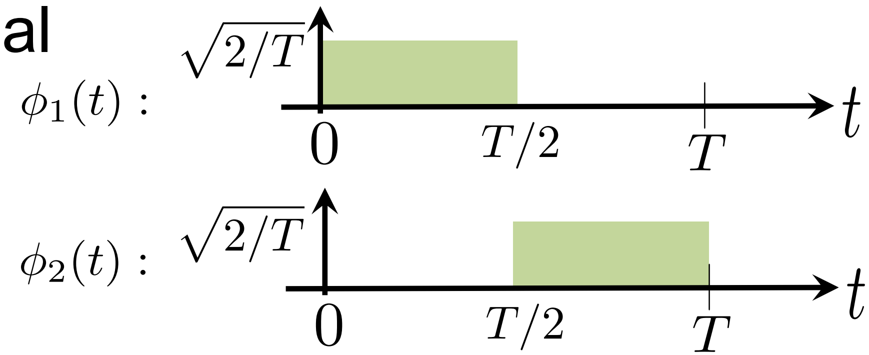
$$N = \int_0^T |E(t)|^2 dt = a^2$$

- Quantum description is a coherent state $|\alpha\rangle$, with $\alpha = \sqrt{N}e^{j\theta} = ae^{j\theta}$
- Classical deterministic field, $E(t) = \alpha\phi(t)e^{j2\pi f_0 t}$

Mode sorting

- Temporally (or spatially) separated, i.e., non-overlapping modes are trivially orthogonal
  - Example:

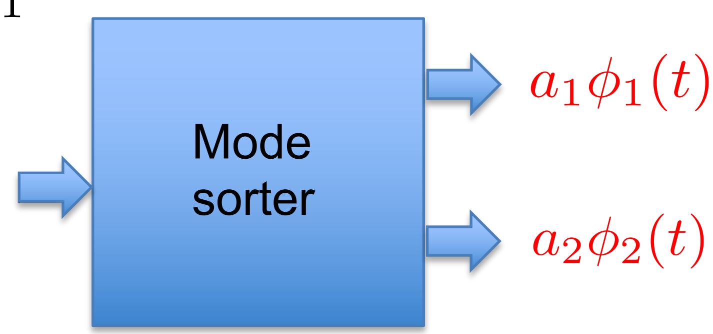
$$\int_0^T \phi_k(t)\phi_l^*(t)dt = \delta_{kl}$$



- Orthogonal modes can be perfectly separated (even if they are overlapping)
- Consider an orthogonal mode basis with K = TW functions

$$\phi_k(t), k = 1, \ldots K \;, E(t) = \sum_{k=1}^{K} a_i \phi_i(t)$$

$$E(t) = a_1\phi_1(t) + a_2\phi_2(t) + 0\phi_3(t) + \ldots$$



Example of overlapping orthogonal modes

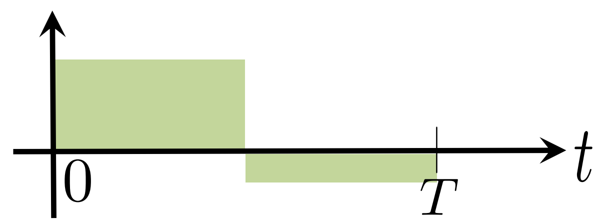
- Orthogonal "chip waveforms" (used in CDMA)

$\phi_1(t)$:

$\phi_2(t)$:

Whenever writing a ket (quantum state), we MUST (implicitly) have a mode in mind

- Consider a coherent state field: $E(t) = a_1\phi_1(t) + a_2\phi_2(t)$



  – In the above mode basis, quantum state: $|a_1\rangle|a_2\rangle$
  – Express the quantum state of this in the non-overlapping mode basis of the previous slide

Problem 1

Hermite Gaussian (HG) modes

- Consider the one dimensional infinite HG basis

$$\phi_q(x) = \left(\frac{1}{2\pi\sigma^2}\right)^{1/4} \frac{1}{\sqrt{2^q q!}} H_q\left(\frac{x}{\sqrt{2}\sigma}\right) \exp\left(-\frac{x^2}{4\sigma^2}\right) \;;x \in \mathbb{R}, q = 0, 1, \ldots, \infty$$

  - $H_q(x)$: Hermite polynomials
  - The q=0 function is the Gaussian: $\phi_0(x) = \left(\frac{1}{2\pi\sigma^2}\right)^{1/4} e^{-x^2/4\sigma^2}$
  - Consider the coherent state of the q=0 mode with mean photon number N and phase 0; $|\sqrt{N}\rangle|0\rangle|0\rangle\ldots$

- Consider the coherent state of $\phi_0(x-a)$, the shifted Gaussian mode (mean photon number N and phase 0)
  - Can you express this coherent state in the HG mode basis?

Problem 2

Laser light pulse

- Quasi-mono-chromatic laser light pulse: in √(photons/m^2-sec) units

$$\tilde{E}(\boldsymbol{r},t) = E(\boldsymbol{r},t)e^{-j\omega_0 t+\phi}, t \in (0,T], \boldsymbol{r} \in \mathcal{A}$$

$$= \psi(\boldsymbol{r})s(t)e^{-j\omega_0 t+\phi}, \ \boldsymbol{r} \equiv (x,y)$$

Spatial and temporal dependence may not be factorable in general

Spatial mode — $\psi(\boldsymbol{r})$

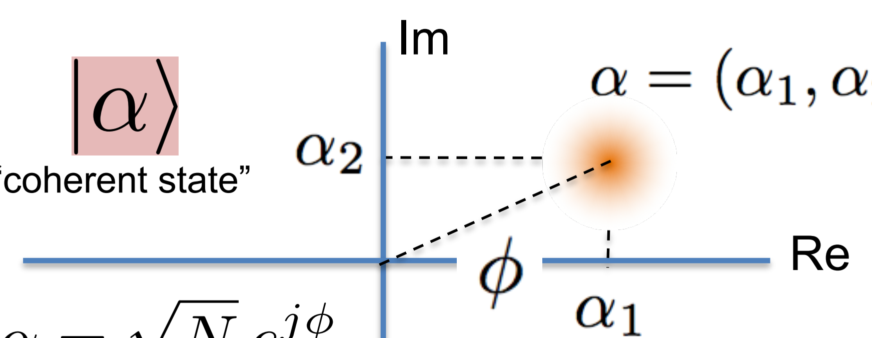
Temporal mode — $s(t)$

- Mean photon number, $N = \int_0^T \int_{\mathcal{A}} |\tilde{E}(\boldsymbol{r},t)|^2 d\boldsymbol{r}dt$

$$= \int_0^T \int_{\mathcal{A}} |E(\boldsymbol{r},t)|^2 d\boldsymbol{r}dt$$

$|\alpha\rangle$

“coherent state”



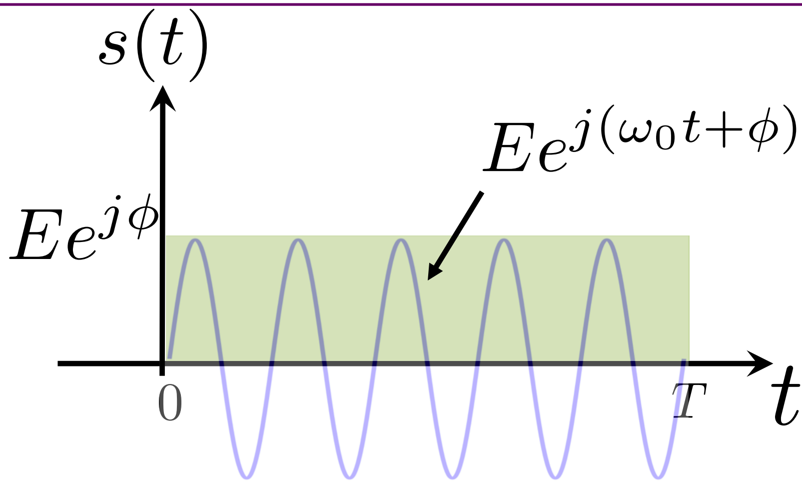
$\alpha = \sqrt{N}\, e^{j\phi}$

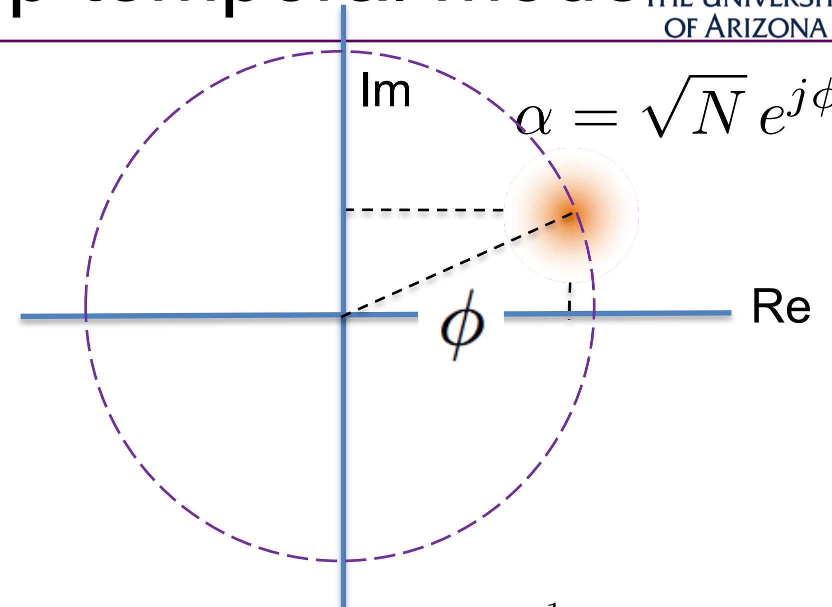
$N = |\alpha|^2$

Phase space picture: once we identify a spatio-temporal-polarization mode, a complex number describes the state of the laser pulse

No detector can accurately measure the field $E(\boldsymbol{r},t)$

Coherent state of a flat-top temporal mode





$$\phi(t) = \begin{cases} \frac{1}{\sqrt{T}}, & t \in [0,T) \\ 0, & \text{otherwise} \end{cases}$$

Ideal direct detection produces a PPP of rate

$$\lambda(t) = |s(t)|^2 = \lambda = E^2, t \in (0,T]$$

$N = \int_0^T \lambda(t)dt = \lambda T = E^2 T$ = mean photon number in mode

ϕ = carrier phase

$\alpha = \sqrt{N}\, e^{j\phi}$ = photon-number unit complex field, i.e., $|\alpha|^2 = N$

Mode: $\phi(t) = \frac{s(t)}{\sqrt{N}}$, normalized spatio-temporal “shape” of field $\int_0^T \phi(t)\phi^*(t)dt = 1$

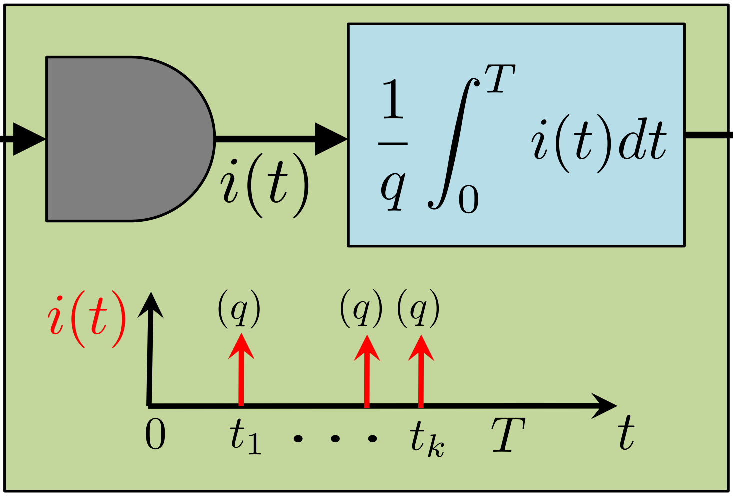
Mode $\phi(t)$, a quantum system, is excited in a coherent state $|\alpha\rangle$

Ideal photon detection on a laser pulse

- Poisson point process (PPP) with rate, $\lambda(t) = |s(t)|^2$
  - For constant rate PPP, interarrival time is exponentially distributed
    $p(\tau) = \lambda e^{-\lambda\tau}, \tau \geq 0$

Probability of one arrival in a Δt interval, $p = \lambda \, \Delta t$

$$s(t)e^{-j\omega_0 t+\phi}, t \in (0, T]$$



$$k$$

$$N = \int_0^T \lambda(t)dt$$ Mean photon number

$$P_K[k] = \frac{e^{-N} N^k}{k!}, k \in \mathbb{Z}$$

Direct detection has no information about the phase, ϕ

Quantization of the field

- Classical (deterministic) field (coherent state)

$$E(t) = \sum_{k=1}^{K} a_i \phi_i(t)$$

- Quantum description of the field: $\hat{E}(t) = \sum_{k=1}^{K} \hat{a}_i \phi_i(t)$
  - Field becomes an operator
  - Field described by a quantum state of constituent modes
  - Modal annihilation operator: $\hat{a}_i$
  - Classical field is a special case: each mode i is excited in a coherent state $|\alpha_i\rangle$, $\alpha_i = a_i$
  - Classical statistical field is a mixture of coherent states, density operator $\rho = \int P(\boldsymbol{\alpha})|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|d\boldsymbol{\alpha}$, $|\boldsymbol{\alpha}\rangle = |\alpha_1\rangle|\alpha_2\rangle \ldots |\alpha_K\rangle$

Upcoming topics…

- Review of single mode quantum optics
  - Annihilation and creation operations, Density operators, phase space, Characteristic functions, Wigner functions, Entanglement
  - Squeezed states of light