



# Quantum Computing and Signal Processing

David A. Meyer

*Project in Geometry and Physics, Department of Mathematics  
University of California/San Diego, La Jolla, CA 92093-0112 USA*  
dmeyer@math.ucsd.edu; <http://math.ucsd.edu/~dmeyer>

Internet Statistics and Metrics Analysis  
Workshop on Internet Signal Processing  
San Diego Supercomputer Center  
12 November 2004



# Outline

quantum *versus* classical information theory

quantum key distribution

Shor's quantum factoring algorithm

the signal processing problem inside the factoring algorithm

a quantum template matching algorithm

conclusions

## Information theory

*We wish to consider certain general problems involving communication systems. To do this it is first necessary to represent the various elements involved as mathematical entities, suitably idealized from their physical counterparts.*

[Shannon 1948]

A **bit** is an element of  $\mathbb{Z}_2$ .

A probability measure on  $\mathbb{Z}_2$  describes a bit produced by a stochastic source:

$$\mathbb{R}^2 \ni \mu = p|0\rangle + (1-p)|1\rangle, \quad 0 \leq p \leq 1.$$

So a **bit** is a non-negative vector in  $\mathbb{R}^2$  with unit  $L_1$ -norm.

# Information theory

*Information is physical.*

[Landauer 1991]

... and quantum systems can instantiate quantum information.

Isolated quantum systems are represented by unit  $L_2$ -norm vectors in complex vector spaces.

In dimension 2, we have a qubit:

$$\mathbb{C}^2 \ni \psi = \psi_0|0\rangle + \psi_1|1\rangle, \quad |\psi_0|^2 + |\psi_1|^2 = 1.$$

A (complete von Neumann) measurement is a choice of basis. The outcome of a measurement is one of the basis vectors; it is  $|b\rangle$  with probability  $|\psi_b|^2$ .

Isolated quantum systems evolve unitarily:  $\psi \mapsto U\psi$ .

## Example

Suppose  $A$  prepares a qubit in the state  $|0\rangle$  and sends it to  $B$ .

If there is no noise in the channel and  $B$  measures the qubit in the basis  $\{|0\rangle, |1\rangle\}$ , the outcome will be  $|0\rangle$  with probability 1.

Now suppose  $A$  prepares a qubit in the state  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  and sends it to  $B$ .

Even if there is no noise in the channel, if  $B$  measures in the basis  $\{|0\rangle, |1\rangle\}$ , the outcome will be  $|0\rangle$  with probability  $\frac{1}{2}$  and  $|1\rangle$  with probability  $\frac{1}{2}$ .

Only if  $B$  measures in the basis  $\{|+\rangle, |-\rangle\}$ , where  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ , will the outcome be deterministic, *i.e.*,  $|+\rangle$  with probability 1.

## Quantum key distribution [Bennett & Brassard 1984]

Suppose  $A$  has two private strings  $x$  and  $a$  of  $4n$  i.i.d. random bits each, with each bit equally likely to be 0 or 1.

$A$  encodes each bit in  $x$  as a qubit in the state  $|0\rangle$  or  $|1\rangle$  if the corresponding bit in  $a$  is 0, and as  $|+\rangle$  or  $|-\rangle$  if the corresponding bit in  $a$  is 1, and sends the qubits to  $B$ .

Suppose  $B$  also has a private random string  $b$  of  $4n$  bits, and measures the qubits one at a time using either the basis  $\{|0\rangle, |1\rangle\}$  or the basis  $\{|+\rangle, |-\rangle\}$ , according to whether the corresponding bit of  $b$  is 0 or 1.

$B$  announces when he finishes, and then  $A$  announces  $a$ .  $B$  discards all the measurement outcomes where he used the wrong measurement basis, and announces which set of bits he discarded.

The remaining  $\approx 2n$  bits that  $B$  has measured are the same as the corresponding bits that  $A$  encoded.

## Security of quantum key distribution

To check that their shared bits are **private**,  $A$  chooses a random subset of  $n$  bits and announces the set and the values of the bits.

If too many disagree with  $B$ 's measurements,  $B$  announces that fact and the protocol fails. Otherwise the  $\approx n$  remaining bits are private with high probability.

Why? Because any information an adversary might have gained about the qubits as they were sent would have disturbed their state.

Notice that this also implies that the “passive measurements” desired for non-intrusive packet-tracing would be impossible in a quantum network.

## Security of quantum key distribution

*Idea of proof.* Suppose it did not. Consider a single qubit that  $A$  sends, which could be in the state  $|0\rangle$  or in the state  $|+\rangle$ , for example. W.l.o.g. we suppose the adversary makes some unitary operation on the qubit, together with an auxiliary quantum system, initially in the state  $|\phi\rangle$ . Then since the qubit is not disturbed, this unitary operation must act as:

$$\begin{aligned}|0\rangle|\phi\rangle &\mapsto |0\rangle|\phi_0\rangle \\ |+\rangle|\phi\rangle &\mapsto |+\rangle|\phi_+\rangle.\end{aligned}$$

But unitary operations preserve inner products, so

$$\langle 0|+\rangle\langle\phi|\phi\rangle = \langle 0|+\rangle\langle\phi_0|\phi_+\rangle.$$

Since  $\langle 0|+\rangle \neq 0$ , this implies that  $\langle\phi_0|\phi_+\rangle = 1$ , *i.e.*, **no measurement of her auxiliary system gives the adversary any information about the state of the qubit.**

## Vernam cypher

A shared private random  $n$ -bit string  $s$  allows secure communication of an  $n$ -bit message  $m$ :

$A$  encodes the message as  $m + s \in \mathbb{Z}_2^n$  and sends it to  $B$ .

$B$  decodes the message by adding  $s$ , since  $m + s + s = m \in \mathbb{Z}_2^n$ .

The encoded message is a random  $n$ -bit string, so the adversary learns nothing from it.

So quantum mechanics enables secure classical communication.

Quantum networks for secure quantum key distribution have been built, and are even being marketed.

# Factoring

Much of current encryption is based on the (presumed) difficulty of factoring numbers with only large prime factors.

The best classical algorithm known for factoring  $n$ -bit numbers has computational complexity  $O(\exp(cn^{1/3} \log^{2/3} n))$ , which is impractical for large  $n$ .

But **Shor's** algorithm for factoring has computational complexity  $O(n^2 \log n \log \log n)$ , which is practical for **much** larger  $n$ , **provided that a quantum computer can be built.**

## Shor's algorithm

Shor's algorithm is based on the fact that if  $N$  is an  $n$ -bit composite number and  $x$  is a nontrivial solution of  $x^2 \equiv 1 \pmod{N}$ , then at least one of  $\text{g.c.d.}(x - 1, N)$  and  $\text{g.c.d.}(x + 1, N)$  is a nontrivial factor of  $N$ .

So an algorithm to find a factor of  $N$  is:

1. Pick a random integer  $1 < x < N$ . If  $\text{g.c.d.}(x, N) \neq 1$ , done.
2. Find the **period**  $t$  of the function  $r \mapsto x^r$ .
3. If  $t$  is even and  $x^{t/2} \not\equiv -1 \pmod{N}$ , compute  $\text{g.c.d.}(x^{t/2} - 1, N)$  and  $\text{g.c.d.}(x^{t/2} + 1, N)$ ; at least one is a nontrivial factor of  $N$ .

With probability close to  $\frac{1}{2}$ , the condition in step **3** is satisfied, so repeating steps **1–3** a constant number of times finds a factor of  $N$  with high probability.

## Shor's algorithm

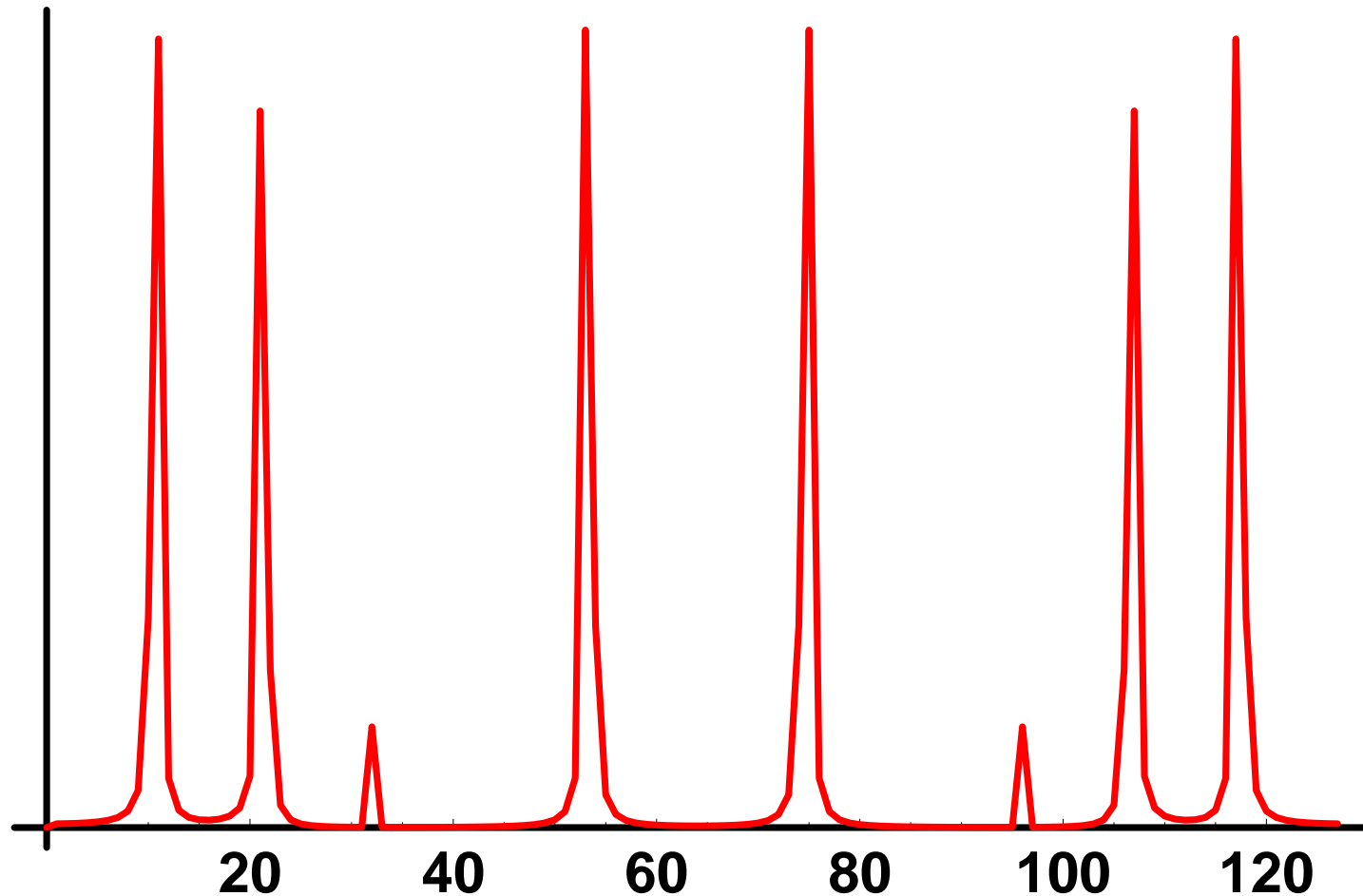
Euclid's algorithm calculates the g.c.d.s in steps **1** and **3** with computational complexity  $O(n^3)$ .

But this is not an efficient **classical** algorithm because step **2** seems to have computational complexity  $O(N)$ .



## Period finding

Taking the discrete Fourier transform gives:



where the points representing the norm-squareds of the components have been connected for better visualization.

## Period finding

The first peak is at 11, which implies a period of  $t = \lfloor 128/11 \rfloor = 12$ .

This period is even, so we compute  $\text{g.c.d.}(5^6 + 1, 91) = 13$  and  $\text{g.c.d.}(5^6 - 1, 91) = 7$ .

These are the two factors of 91.

## The quantum Fourier transform

Classically, the fast Fourier transform has complexity  $O(N \log N)$ , so this method of finding the period of  $r \mapsto x^r \pmod{N}$  is exponential in the size of the problem,  $n = \log N$ .

But, using the same recursive structure that allows the Fourier transform to be computed fast classically, a quantum computer can compute it with computational complexity  $O((\log N)^2)$  when the data is encoded as the components of a unit  $L_2$ -norm vector in  $\mathbb{C}^N$ .

The only access to the components of the quantum Fourier transformed data is *via* measurement, *i.e.*, we can only sample the probability distribution over basis states defined by the norm-squareds of their components.

This suffices for period finding—in any context—since we only need to find a peak.

# Template matching

A **template** is a map  $g : T = \mathbb{Z}_m \rightarrow \mathbb{Z}_p$ , where  $m$  is the length of the template and  $p$  is the number of values into which the range of the signal is discretized.

A **signal** is a map  $f : S = \mathbb{Z}_M \rightarrow \mathbb{Z}_p$ , where  $M > m$  is the length of the signal and there is some **offset**  $a \in S$  such that for all  $x \in T$ ,  $f(a + x) = g(x)$ , *i.e.*, the template occurs as a subsignal of the signal.

The **TEMPLATE MATCHING** problem is: given  $f$ , determine the offset  $a$  of the template in the signal.

And, of course, we really want to be able to solve this problem in the presence of noise.

## Correlation

Compare the template and a region of the signal using the **correlation** between the sets of corresponding values:

$$\text{Corr}[g, f](y) = \frac{\sum_{x \in T} (g(x) - \hat{g}) (f(y + x) - \hat{f}(y))}{\sqrt{\sum_{x \in T} |g(x) - \hat{g}|^2} \sqrt{\sum_{x \in T} |f(y + x) - \hat{f}(y)|^2}},$$

where  $y \in I$ , and  $\hat{g}$  and  $\hat{f}(y)$  are the average values:

$$\hat{g} = \frac{1}{|T|} \sum_{x \in T} g(x) \quad \text{and} \quad \hat{f}(y) = \frac{1}{|T|} \sum_{x \in T} f(y + x).$$

At an offset  $y$  such that  $f(y + x) = g(x)$  for all  $x \in T$ ,  $\text{Corr}[g, f](y) = 1$ . Also, by the Cauchy-Schwarz inequality,  $|\text{Corr}[g, f](y)| \leq 1$  for all  $y \in I$ .

## A classical solution

This implies a classical *Correlation Algorithm* for TEMPLATE MATCHING:

1. compute  $\text{Corr}[g, f](y)$  for all  $y \in S$ ;
2. locate the maxima of the correlation function;
3. return these offsets as the loci of the template in the signal.

## Classical complexity

For fixed  $y$ , calculating  $\text{Corr}[g, f](y)$  has complexity  $O(|T|)$ , so calculating the correlation one argument at a time has complexity  $O(|S||T|)$ .

We can extend (pad)  $g$  to a function  $\tilde{g} : S \rightarrow \mathbb{Z}_p$  such that  $\tilde{g}|_T = g$  and  $\tilde{g}|_{S \setminus T} = 0$ .

Letting  $\chi_T$  be the characteristic function for the region  $T$  in  $S$ , the numerator of the correlation becomes:

$$\begin{aligned} \sum_{x \in T} (\overline{g(x) - \hat{g}}) f(y + x) &= \sum_{x \in S} (\overline{\tilde{g}(x) - \chi_T(x)\hat{g}}) f(y + x) \\ &= \mathcal{F}_S^{-1} \left[ \overline{\mathcal{F}_S[\tilde{g} - \chi_T\hat{g}] \mathcal{F}_S[f]} \right] (y), \end{aligned}$$

which can be calculated for all  $y$  with complexity  $O(|S|\log|S|)$  using the FFT to calculate  $\mathcal{F}_S$  and  $\mathcal{F}_S^{-1}$ . Hence the classical computational complexity of the *Correlation Algorithm* is  $O(\min\{|S|\log|S|, |S||T|\})$ .

## A quantum solution [Curtis & Meyer 2004]

Since we are looking for a peak in  $\text{Corr}[g, f](y)$ , this should be a signal processing problem to which we can apply the quantum Fourier transform, followed by measurement.

There is a quantum algorithm for TEMPLATE MATCHING in which the measurement samples from the probability distribution on  $S$  defined by:

$$\frac{1}{|S|} \left| \mathcal{F}_S^{-1} \left[ \frac{\overline{\mathcal{F}_S[\tilde{g}]}}{|\mathcal{F}_S[\tilde{g}]|} \mathcal{F}_S[f] \right] (y) \right|^2,$$

which is similar to the norm-squared of  $\text{Corr}[g, f](y)$ .

The quantity being computed is essentially the **phase-only correlation**.

## A quantum solution [Curtis & Meyer 2004]

This computational complexity of this algorithm is  $O((\log|S|)^2)$  once the signal has been acquired.

For **random** signals, the success probability satisfies:

$$\lim_{|S| \rightarrow \infty} \frac{|S|}{|T|} \text{prob}(\text{correct offset}) = \frac{\pi}{4}.$$

## Conclusions

There will eventually be a quantum internet, if only for secure key distribution.

Measurement will be an even more difficult problem than it already is for the Internet.

Physicists and engineers are working hard to build special and general purpose quantum computers.

If one is built, it will be able to compute Fourier transforms faster than fast, and hence will be able to solve certain signal processing problems efficiently.

Mathematicians and computer scientists are working hard to develop other quantum transforms (the Haar wavelet transform is easy, for example) and algorithms.