Towards quantum template matching

Daniel Curtis and David A. Meyer

Department of Mathematics, University of California/San Diego, La Jolla, CA 92093-0112

ABSTRACT

We consider the problem of locating a template as a subimage of a larger image. Computing the maxima of the correlation function solves this problem classically. Since the correlation can be calculated with the Fourier transform this problem is a good candidate for a superior quantum algorithmic solution. We outline how such an algorithm would work.

Keywords: image processing, Fourier transform, phase-only correlation.

1. INTRODUCTION

The current breadth of interest in quantum computation originates primarily from Shor's discovery of a quantum algorithm for factoring[1]. This algorithm is more efficient—*i.e.*, requires asymptotically fewer logical operations as the size of the problem increases—than the best classical algorithm known[2], which inspires the hope that there are superior quantum algorithms for other classical problems. Subsequent discoveries of quantum algorithms for unstructured[3] and structured[4,5,6,7,8] search, for the shifted Legendre symbol problem[9], and for solutions to Pell's equation[10] have nourished this hope. None of these problems has the practical relevance of factoring, however, upon the classical difficulty of which the security of modern cryptosystems rests[11]. Quantum algorithms for other practical problems would help justify the immense commitment of resources that seems likely to be required to develop a working quantum computer.

All of the known quantum algorithms exploit the fact that there are quantum gate arrays for the Fourier transform with complexity exponentially smaller than that of even the Fast Fourier Transform (FFT)[1,12]. (The so-called Hadamard transform, H, of a single qubit is the 2-dimensional discrete Fourier transform; acting in parallel on n qubits, as it does in many of these algorithms[13], $H^{\otimes n}$ is the Fourier transform over the group $\mathbb{Z}_2^n$. It also has exponentially smaller quantum than classical complexity.) The Fourier transform, of course, is ubiquitous in signal processing, which suggests that there should be efficient quantum algorithms in this problem domain[14]. Since quantum state amplitudes are accessible only by sampling, however, a classical algorithm must solve a signal processing problem by identifying a peak in a Fourier transform in order to be a candidate for quantum speed-up. Nevertheless, the Bernstein-Vazirani algorithm[4] can be interpreted as a quantum algorithm for efficiently decoding signals encoded using the simplex code[15]; it uses the Hadamard transform, $H^{\otimes n}$.

In the context of image processing, it is the 2D Fourier transform that naturally arises; like the 1D Fourier transform, the quantum version is exponentially more efficient than any fast classical implementation. We are thus led to search for quantum image processing algorithms. Here we consider one particular image processing task that can be solved classically by using the FFT: template matching. In §2 we specify this problem precisely, and in §3 describe a classical algorithm that solves the problem. This algorithm calculates the maximum of a function computed using the 2D Fourier transform, which, by the preceding discussion,

---

Email: dcurtis@math.ucsd.edu, dmeyer@math.ucsd.edu

suggests that it might have a quantum version. And in §4 we derive a quantum version of this classical algorithm. In §5 we conclude with a discussion, explaining what needs to be done to convert this into a quantum algorithm for template matching.

2. THE PROBLEM

Suppose there is some object that we would like to be able to locate in any given image. For example, Figure 1 shows one specific view of a truck; it is a grayscale image, *i.e.*, a map $g : T = \mathbb{Z}_m \times \mathbb{Z}_n \rightarrow \mathbb{Z}_p$, where typically $p = 256$. In the problem that we are considering, such a map is called a *template*. In the simplest version of this problem the set of possible images consists of

Figure 1. An aerial photograph of a truck.

larger images that *contain the template as a subimage, i.e.*, they are maps $f : I = \mathbb{Z}_M \times \mathbb{Z}_N \rightarrow \mathbb{Z}_p$ such that for some $a \in I$ and all $x \in T$, $f(a + x) = g(x)$. Figure 2 is an example of an image that contains the template shown in Figure 1. The TEMPLATE MATCHING problem is: given f, determine the *offset a*.

Figure 2. An aerial image including the truck shown in Figure 1.

In the next section we describe an algorithm that solves TEMPLATE MATCHING classically. Before doing so, however, we emphasize that it is *only* this problem that we address in this paper. There are many other ways that an object might be specified: by a collection of templates, by some 3D description, *etc.* There are also many other sets of possible images: the template might be noisy or partially obscured, it might occur

rotated or scaled or from another viewpoint, *etc.* These are all important, real-world situations that lead to challenging image processing problems, not all of which have known classical solutions. Here we concentrate on the simplest template matching problem; the lessons learned in deriving a quantum version of a classical algorithm that solves this problem should inform the derivation of quantum versions of classical algorithms for more complicated template matching problems.

3. A CLASSICAL SOLUTION

To compare the template with a region in an image one can compute the *correlation*[16] between the sets of corresponding pixel values:

$$\text{Corr}[g, f](y) = \frac{\sum_{x \in T} \overline{(g(x) - \hat{g})} \left(f(y + x) - \hat{f}(y)\right)}{\sqrt{\sum_{x \in T} |g(x) - \hat{g}|^2} \sqrt{\sum_{x \in T} |f(y + x) - \hat{f}(y)|^2}}, \tag{3.1}$$

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

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

The definition (3.1) allows for the possibility that the function values are complex; this will be relevant in the next section.

Notice that at an offset y such that $f(y + x) = g(x)$, the numerator and the denominator in (3.1) are the same, so $\text{Corr}[g, f](y) = 1$. Also, by the Cauchy-Schwarz inequality, $|\text{Corr}[g, f](y)| \leq 1$ for all $y \in I$. Thus, calculating the correlation function, taking its absolute value, and finding the maxima, identifies offsets at which the template exactly matches a region of the image. If the pixel values $f(x)$, $x \in I$ were i.i.d. random variables with $g(x) = f(a + x)$, $x \in T$, then the expected value of $\text{Corr}[g, f](y)$ would be 0 except at $y = a$, where it would be 1. In a real image, however, the pixel values are not independent since pixels near each other tend to have similar values, while pixels far from each other tend to be less correlated. This implies that $\text{Corr}[g, f](y)$ should have larger (than zero) values for y near a. Figure 3 shows that this is indeed the case for the template and image of Figures 1 and 2; the maximum occurs at the tip of an ellipsoidal peak with eccentricity and orientation corresponding to the aspect ratio of the template.

For a fixed y, calculating the right hand side of (3.1) has complexity $O(|T|)$. Since there are $|I|$ possible y's, calculating the correlation function one argument at a time has classical complexity $O(|I||T|)$. Notice, however, that we can extend (pad) g to a function $\tilde{g} : I \to \mathbb{Z}_p$ such that $\tilde{g}|_T = g$ and $\tilde{g}|_{I \setminus T} = 0$. Expanding and simplifying the numerator of (3.1) gives

$$\sum_{x \in T} \overline{(g(x) - \hat{g})} f(y + x) = \sum_{x \in I} \overline{(\tilde{g}(x) - \chi_T(x)\hat{g})} f(y + x), \tag{3.2}$$

where χ_T is the characteristic function for the region T in I. Evaluating the right hand side of (3.2) for a fixed y has complexity $O(|I|)$, but it can be calculated for all arguments y with complexity less than $O(|I|^2)$:

$$\sum_{x \in I} \overline{(\tilde{g}(x) - \chi_T(x)\hat{g})} f(y + x) = \mathcal{F}_I^{-1} \left[\overline{\mathcal{F}_I[\tilde{g} - \chi_T \hat{g}]} \mathcal{F}_I[f]\right](y),$$

which has complexity $O(|I| \log |I|)$ if the Fourier transforms $\mathcal{F}_I$ are calculated using the FFT. Since the second factor in the denominator of (3.1) can be calculated similarly, the classical computational complexity of this solution is $O(\min\{|I| \log |I|, |I||T|\})$.

Figure 3. The correlation function computed for the truck template and the image shown in Figure 2. Lighter grayscale indicates larger values. There is a unique maximum, at the offset corresponding to the location of the template in the image.

4. A QUANTUM VERSION

As we posed the TEMPLATE MATCHING problem in §2, f and g are grayscale images, *i.e.*, arrays of $\mathbb{Z}_p$ values, typically with $p = 256$. For the quantum version of the correlation algorithm, we transform the functions as follows: Let $\omega = e^{2\pi i/p}$ and let $F = \omega^f$, $G = \omega^g$. Maxima of the absolute value of the correlation of F and G occur at the same offsets as they do for f and g, but the computation is simpler to approximate: If the pixel values in the image were i.i.d. random variables uniformly distributed over the range of possible values, then the expectation values of both $\hat{F}(y)$ and $\hat{G}$ would be 0. Thus, the expectation value of the numerator of the correlation would be just $\sum_{x \in T} \overline{G(x)} F(y + x)$. Similarly, the expectation value of the denominator would be $|T|$, since each term in the sums would be the norm-squared of a unit complex number. Thus we have the approximation that

$$\text{Corr}[G, F](y) \approx \frac{1}{|T|} \sum_{x \in T} \overline{G(x)} F(y + x) = \frac{1}{|T|} \mathcal{F}_I^{-1} \left[\overline{\mathcal{F}_I[\tilde{G}]} \mathcal{F}_I[F] \right](y), \tag{4.1}$$

where the ˜ again denotes that G has been padded with 0's on the domain $I \setminus T$. Figure 4 shows that this approximation is relatively good.

The quantum version of the correlation algorithm will evaluate the right hand side of (4.1), using the fact that the Fourier transforms can be computed more efficiently quantum mechanically[1,12] to reduce the computational complexity below $O(|I| \log |I|)$. This is not completely straightforward, however, since we want
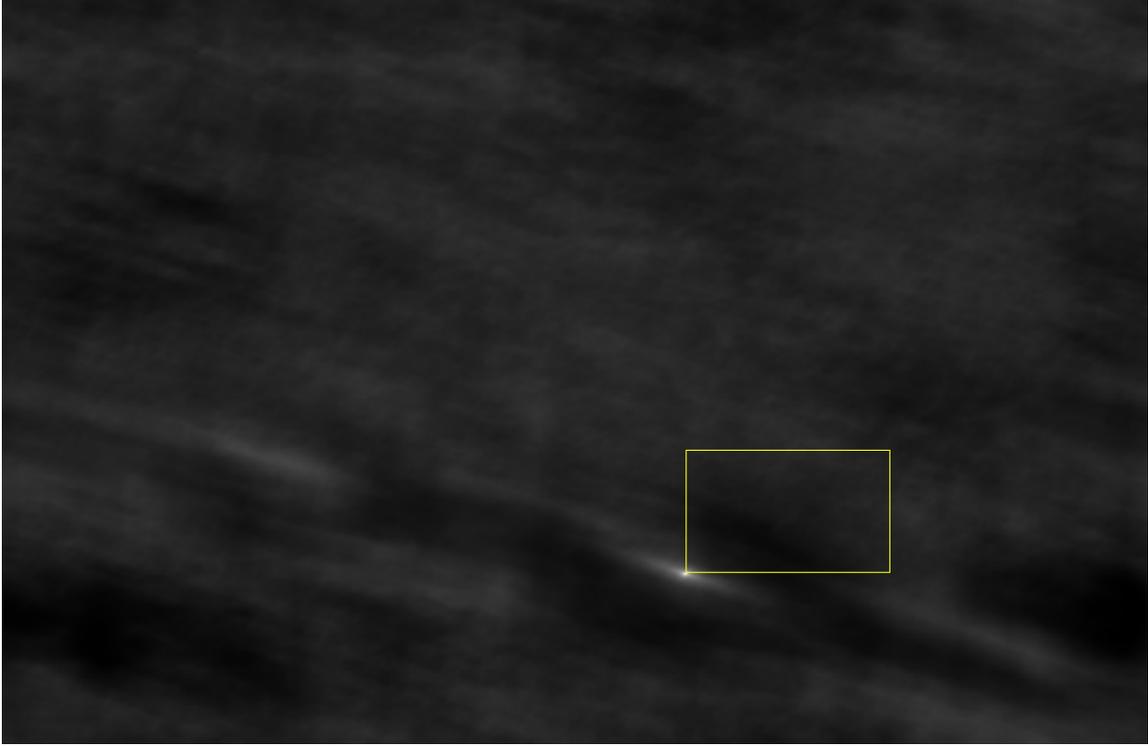
Figure 4. The approximate correlation function (4.1), again computed for the truck template and the image shown in Figure 2. Lighter grayscale indicates larger values. Although there is more variation than in Figure 3, there is still a unique maximum, at the offset corresponding to the location of the template in the image.

to compute two discrete Fourier transforms and multiply them component-wise; since quantum computers cannot multiply the corresponding components of two state vectors, this must be done asymmetrically.

Thus, instead of preparing two state vectors, one for F and one for G, we only prepare a state vector representing the image: Let

$$|\omega\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \varpi^k |k\rangle,$$

and define a unitary operation U_f acting on $\mathbb{C}^{|I|} \otimes \mathbb{C}^p$ by

$$U_f |x\rangle |c\rangle = |x\rangle |c + f(x)\rangle.$$

To prepare the state vector representing the image we use 'phase kickback'[17]:

1. Initialize the quantum system to the state $|0\rangle |0\rangle \in \mathbb{C}^{|I|} \otimes \mathbb{C}^p$.

2. Apply $\mathcal{F}_I^{-1} \otimes \mathcal{F}_p^{-1} X_p$ to obtain the state $\dfrac{1}{\sqrt{p|I|}} \sum_{x \in I} |x\rangle |\omega\rangle$. ($X_p |c\rangle = |c + 1\rangle$ is the p-dimensional analogue of the Pauli matrix σ_x.)

3. Apply U_f to obtain the state $\dfrac{1}{\sqrt{p|I|}} \sum_{x \in I} \omega^{f(x)} |x\rangle |\omega\rangle = \dfrac{1}{\sqrt{p|I|}} \sum_{x \in I} F(x) |x\rangle |\omega\rangle$.

Next, to compute its Fourier transform we:

4. Apply $\mathcal{F}_I \otimes \mathrm{id}_p$ to obtain the state $\dfrac{1}{\sqrt{p|I|}} \displaystyle\sum_{u \in I^*} \mathcal{F}_I[F](u)|u\rangle|\omega\rangle$. ($I^*$ is the dual space to I, on which the Fourier transform of F is defined. id_p is the p-dimensional identity matrix.)

To represent the operation of component-wise multiplication by the conjugate of the Fourier transform of $\tilde{G}$, we would like to multiply by a diagonal matrix with diagonal elements these components. To be a step in a quantum algorithm, however, this matrix would have to be unitary, *i.e.*, each diagonal element would have to have norm 1. So we define V_g to be the diagonal matrix with diagonal elements $\overline{\mathcal{F}_I[\tilde{G}](u)}/|\mathcal{F}_I[\tilde{G}](u)|$. Then the next step is to:

5. Apply $V_g \otimes \mathrm{id}_p$ to obtain the state $\dfrac{1}{\sqrt{p|I|}} \displaystyle\sum_{u \in I^*} \dfrac{\overline{\mathcal{F}_I[\tilde{G}](u)}}{|\mathcal{F}_I[\tilde{G}](u)|} \mathcal{F}_I[F](u)|u\rangle|\omega\rangle$.

Finally, we:

6. Apply $\mathcal{F}_I^{-1} \otimes \mathrm{id}_p$ to obtain the state $\dfrac{1}{\sqrt{p|I|}} \displaystyle\sum_{y \in I} \mathcal{F}_I^{-1}\left[\dfrac{\overline{\mathcal{F}_I[\tilde{G}]}}{|\mathcal{F}_I[\tilde{G}]|} \mathcal{F}_I[F] \right](y)|y\rangle|\omega\rangle$.

7. Measure the state in the pixel basis to obtain y with probability $\dfrac{1}{p|I|}\left| \mathcal{F}_I^{-1}\left[\dfrac{\overline{\mathcal{F}_I[\tilde{G}]}}{|\mathcal{F}_I[\tilde{G}]|} \mathcal{F}_I[F] \right](y) \right|^2$.

Were it not for the normalization by $|\mathcal{F}_I[\tilde{G}]|$, these probabilities would be proportional to the norm-squared values on the right hand side of (4.1). Figure 5 shows the results of this 'phase-only correlation' algorithm; the probability of observing $y = a$ is 0.00473. For comparison, if the exact correlations of (3.1) are normalized to be probabilities, *i.e.*, so that their norm-squares sum to one, the maximum is only 0.000681. In this sense the 'phase-only correlation' algorithm is *better* than the correlation algorithm. Although we have been led to this algorithm by the requirement of unitarity for a quantum algorithm, it has also been discovered as a classical algorithm[18]. The Fourier transforms have classical complexity $O(|I|\log|I|)$ and quantum complexity $O\big((\log|I|)^2\big)$, so there is an exponential improvement in the processing of the image, once it has been input, *i.e.*, after steps **1–3**.

5. DISCUSSION

The quantum algorithm defined by steps **1–7** in §4 is not a complete solution to TEMPLATE MATCHING. Although at the end of step **6** the amplitude of $|y\rangle$ in the state vector is the 'phase-only correlation' at y, in step **7** we are only *sampling* the probability distribution. Although the probability of observing $y = a$ is larger than the probability of observing any other y value, it is still relatively small. To increase the probability of success, we must *amplify* this probability. Classically, this entails repeating steps **1–7** multiple times, and taking as the output the most commonly observed y value. Quantum mechanically, the probability can be increased by not implementing step **7**, but rather applying the technique of *amplitude amplification*[19,20]. We are currently investigating in which situations each of these protocols can be successfully implemented and solve the problem with computational complexity less than the classical correlation algorithm we described in §3.

Figure 5. The 'phase-only correlation' function, again computed for the truck template and the image shown in Figure 2. Lighter grayscale indicates larger values. There is a unique maximum, more pronounced than in Figures 3 and 4, at the offset corresponding to the location of the template in the image.

ACKNOWLEDGEMENTS

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", in S. Goldwasser, ed., *Proceedings of the 35th Symposium on Foundations of Computer Science*, Santa Fe, NM, 20–22 November 1994 (Los Alamitos, CA: IEEE Computer Society Press 1994) 124–134;
P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J. Comput.* **26** (1997) 1484–1509.

[2] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse and J. M. Pollard, "The number field sieve", in *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, Baltimore, MD, 14–16 May 1990 (New York: ACM Press 1990) 564–572;
A. K. Lenstra and H. W. Lenstra, Jr., eds., *The Development of the Number Field Sieve*, Lecture Notes in Mathematics, vol. 1554 (New York: Springer-Verlag 1993).

[3] L. K. Grover, "A fast quantum mechanical algorithm for database search", in *Proceedings of the*

Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, 22–24 May 1996 (New York: ACM 1996) 212–219.

[4] E. Bernstein and U. Vazirani, "Quantum complexity theory", in *Proceedings of the 25th ACM Symposium on Theory of Computing*, San Diego, CA, 16–18 May 1993 (New York: ACM Press 1993) 11–20; E. Bernstein and U. Vazirani, "Quantum complexity theory", *SIAM J. Comput.* **26** (1997) 1411–1473.

[5] E. Farhi and S. Gutmann, "Quantum mechanical square root speedup in a structured search problem", `quant-ph/9711035`.

[6] L. K. Grover, "Quantum search on structured problems", *Chaos, Solitons & Fractals* **10** (1999) 1695–1705.

[7] N. J. Cerf, L. K. Grover and C. P. Williams, "Nested quantum search and structured problems", *Phys. Rev. A* **61** (2000) 032303/1–14.

[8] T. Hogg, "Highly structured searches with quantum computers", *Phys. Rev. Lett.* **80** (1998) 2473–2476.

[9] W. van Dam, "Quantum algorithms for weighing matrices and quadratic residues", `quant-ph/0008059`.

[10] S. Hallgren, "Polynomial-time quantum algorithms for Pells equation and the principal ideal problem", in *Proceedings of the 34th ACM Symposium on Theory of Computing*, Montreal, Quebec, Canada, 19–21 May 2002 (New York: ACM Press 2002) 653–658.

[11] R. L. Rivest, A. Shamir and L. Adleman, "A method of obtaining digital signatures and public-key cryptosystems", *Commun. ACM* **21** (1978) 120–126.

[12] D. Coppersmith, "An approximate Fourier transform useful in quantum factoring", IBM T. J. Watson Research Report RC 19642 (1994).

[13] D. R. Simon, "On the power of quantum computation", in S. Goldwasser, ed., *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, 20–22 November 1994 (Los Alamitos, CA: IEEE 1994) 116–123; D. R. Simon, "On the power of quantum computation", *SIAM J. Comput.* **26** (1997) 1474–1483.

[14] A. Klappenecker and M. Rötteler, "On the irresistible efficiency of signal processing methods in quantum computing", `quant-ph/0111039`; in R. Creutzburg and K. Egiazarian, eds., *Proceedings of the First International Workshop on Spectral Techniques and Logic Design for Future Digital Systems*, Tampere, Finland, 2–3 June 2000, TICSP **10** (Monistamo, Finland: TTKK 2000) 483–497.

[15] A. Barg and S. Zhou, "A quantum decoding algorithm for the simplex code", in *Proceedings of the 36th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, 23–25 September 1998 (UIUC 1998) 359–365.

[16] See, *e.g.*, J. Shao, *Mathematical Statistics* (New York: Springer-Verlag 1999).

[17] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, "Quantum algorithms revisited", `quant-ph/9708016`; *Proc. Roy. Soc. Lond. A* **454** (1998) 339–354.

[18] J. Wang, L. E. Reinstein, J. Hanley and A. G. Meek, "Investigation of a phase-only correlation technique for anatomical alignment of portal images in radiation therapy", *Physics in Medicine and Biology* **41** (1996) 1045-1058.

[19] G. Brassard and P. Høyer, "An exact quantum polynomial-time algorithm for Simon's problem", `quant-ph/9704027`; in *Proceedings of Fifth Israeli Symposium on Theory of Computing and Systems*, June 1997 (Los Alamitos, CA: IEEE 1997) 12–23.

[20] G. Brassard, P. Høyer, M. Mosca and A. Tapp, "Quantum amplitude amplification and estimation", `quant-ph/0005055`.