Quantum Search for Zeros of Polynomials

Stefan Weigert
HuMP - Hull Mathematical Physics
Department of Mathematics, University of Hull, UK-Hull
s.weigert@hull.ac.uk

May 2003

Abstract

A quantum mechanical search procedure to determine the real zeros of a polynomial is introduced. It is based on the construction of a spin observable whose eigenvalues coincide with the zeros of the polynomial. Subsequent quantum mechanical measurements of the observable output directly the numerical values of the zeros. Performing the measurements is the only computational resource involved.

PACS: 03.67.-a, 03.65Sq

Introduction

Quantum mechanical measurements are a computational resource. Various quantum algorithms use projective measurements at some stage or other to determine the period of a function e.g. [1]. In [2], projective measurements have been assigned a crucial role for a particular scheme of universal quantum computation which requires measurements on up to four qubits. Related schemes have been formulated based on measuring on triples and pairs [3], and finally on pairs of qubits only [4]. Measurements are also an essential part of Grover's search algorithm in order to actually read the result of the computation [5, 6].

A conceptually different strategy has been applied to propose a special-purpose machine which is capable to diagonalize any finite-dimensional hermitean matrix by genuine quantum means, i.e. quantum measurements [7, 8]. In this approach of *quantum diagonalization*, a hermitean matrix is considered as a quantum mechanical observable of an appropriate one-spin system. Projective measurements with a generalized Stern-Gerlach apparatus provide directly the unknown eigenvalues of the matrix which solves the hard part of the diagonalization. In this paper, it will be shown how to find the real zeros of a prescribed polynomial in a similar way, using quantum mechanical measurements.

The quantum search procedure

Consider a polynomial of degree N which is assumed to have N real zeros ζ_n,

$$P(x) = \sum_{n=0}^{N} p_n x^n \,, \quad p_n \in \mathsf{IR} \,, \quad p_N = 1 \,. \tag{1}$$

The assumption $p_N = 1$ is not a restriction since two polynomials $Q(x)$ and $Q(x)/c, c \neq 0$, have the same zeros. The quantum procedure to identify the zeros ζ_n of $P(x)$ consists of two steps. First, one needs to find a hermitean companion matrix C of the polynomial $P(x)$. By construction, its eigenvalues coincide with the unknown zeros of the polynomial $P(x)$. Second, one determines the eigenvalues of the matrix C by a method inspired by the quantum diagonalization of a hermitean matrix. Effectively, they are obtained by measuring the eigenvalues of a quantum mechanical spin observable $\hat{C}$ with matrix representation C.

Hermitean companion matrix of a polynomial

It is straightforward to calculate the characteristic polynomial $P_{\mathsf{M}}(\lambda)$ of an $(N \times N)$ matrix M:

$$\det\left(\mathsf{M} - \lambda \mathsf{E}\right) = P_{\mathsf{M}}(\lambda) \,, \tag{2}$$

where E is the $(N \times N)$ unit matrix. The polynomial $P_{\mathsf{M}}(\lambda)$ has degree N, and its zeros coincide with the eigenvalues $\mu_n, n = 1, \ldots, N$, of the matrix M. Hermitean matrices have real eigenvalues only, hence all zeros of its characteristic polynomial are located on the real axis. The inverse problem reads:

- Given a polynomial $P(x)$ of degree N with real zeros, find a *hermitean* matrix C such that its characteristic polynomial is $P(x)$.

The matrix C is known as *companion* matrix of the polynomial $P(x)$. Obviously, the companion matrix should be determined *without* reference to the roots of the given polynomial. If C is one solution of the inverse problem, then the matrices $\mathsf{C}_{\mathsf{U}} = \mathsf{U}\mathsf{C}\mathsf{U}^{\dagger}$ provide solutions as well, where U is any unitary $(N \times N)$ matrix. The difficult part of the inverse problem lies in the requirement to find a *hermitean* matrix C: it is easy to specify a non-hermitean companion matrix C_0 of the polynomial (1), *viz.*,

$$\mathsf{C}_0 = \begin{pmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ & & & 1 \\ -p_0 & -p_1 & \cdots & -p_{N-1} \end{pmatrix} . \tag{3}$$

Partial solutions of the problem to find hermitean companion matrices have been obtained in [9]. A complete and constructive solution can be found in [10], where a tridiagonal companion matrix C is specified in terms of the coefficients $p_n, n = 0, 1, \ldots, N$. Explicitly, a polynomial $P(x)$ of degree N with N real zeros can be written in the form

$$P(x) = (-)^N \det\left(\mathsf{C} - x\mathsf{E}\right) , \tag{4}$$

where the matrix C is tridiagonal and real symmetric, hence hermitean:

$$\mathsf{C} = \begin{pmatrix} -q_1(0) & \sqrt{d_1} & & & & & \\ \sqrt{d_1} & -q_2(0) & \sqrt{d_2} & & & & \\ & \sqrt{d_2} & -q_3(0) & \ddots & & & \\ & & \ddots & \ddots & & & \\ & & & & -q_{n-2}(0) & \sqrt{d_{n-2}} & \\ & & & & \sqrt{d_{n-2}} & -q_{n-1}(0) & \sqrt{d_{n-1}} \\ & & & & & \sqrt{d_{n-1}} & -q_n(0) \end{pmatrix} . \tag{5}$$

The nonnegative numbers $d_k, k = 1, 2, \ldots, N-1$, and the polynomials $q_n(x), n = 1, 2, \ldots, N$, are generated when applying a *Modified Euclidean Algorithm* [10] to the polynomial $P(x)$. The operations required to determine the matrix elements of C are $(\imath)$ repeated division of polynomials, $(\imath\imath)$ evaluation of specific polynomials at $x = 0$; $(\imath\imath\imath)$ taking square roots of numbers d_k. As a corollary, the Modified Euclidean Algorithm checks whether the given polynomial has real zeros only: if any of the numbers d_k is found to be negative, $P(x)$ can not have real zeros only. For completeness, the algorithm is sketched in the Appendix.

Quantum search for eigenvalues of hermitean matrices

Four steps are necessary to find the eigenvalues of a given hermitean matrix C with N different eigenvalues by means of quantum measurements. Here an outline of this approach will be given only; for details about the procedure for $(N \times N)$ matrices readers should consult [7], while it is illustrated for (2×2) matrices in [8].

The matrix must be $(\imath)$ written in *standard form*; next, it is interpreted as $(\imath\imath)$ matrix representation of a unique *observable* $\hat{C}$ of a quantum spin; this observable can be measured by $(\imath\imath\imath)$ a specific *apparatus* which needs to be identified and built; finally, the apparatus is used to generate the eigenvalues by $(\imath v)$ actually *measuring* the observable C.

$(\imath)$ *Standard form of* C*:* Write the hermitean $(N \times N)$ matrix C as a combination of linearly independent hermitean *multipole* operators $\mathsf{T}_\nu, \nu = 0, \ldots, N^2 - 1$,

$$\mathsf{C} = \sum_{\nu=0}^{N^2-1} c_\nu \mathsf{T}_\nu , \qquad c_\nu = \frac{1}{N} \mathrm{Tr}\ \left[\mathsf{C}\,\mathsf{T}_\nu\right] \in \mathsf{IR} . \tag{6}$$

There are N^2 self-adjoint multipole operators $\hat{T}_\nu = \hat{T}_\nu^\dagger$ with matrix representations T_ν, and they form a basis in the space of hermitean operators acting on an N-dimensional Hilbert space $\mathcal{H}$ [12]. These operators consist of all traceless symmetric products of up to N spin components $\hat{\mathbf{S}} = (\hat{S}_x, \hat{S}_y, \hat{S}_y)$, plus the identity operator. Two multipoles are orthogonal with respect to a scalar product defined as the trace of their product: $(1/N)$ Tr $\left[\hat{T}_\nu \hat{T}_{\nu'}\right] = \delta_{\nu\nu'}$.

(*ii*) *Identification of an observable:* On the basis of the expansion (6) interpret the matrix C as representing an observable $\hat{C}$ for a spin with quantum number $s = (N-1)/2$:

$$\hat{C} = C(\hat{\mathbf{S}}) = \sum_{\nu=0}^{N^2-1} c_\nu \hat{T}_\nu \,, \tag{7}$$

thinking of the multipoles as functions of the spin components, $\hat{T}_\nu = T_\nu(\hat{\mathbf{S}})$.

(*iii*) *Setting up a measuring device for $\hat{C}$:* Swift and Wright have shown in [12] how to devise a *generalized Stern-Gerlach apparatus* which measures any spin observable $\hat{C}$. The construction generalizes the traditional Stern-Gerlach apparatus which measures the spin component $\mathbf{e}_n \cdot \hat{\mathbf{S}}$ along a direction specified by a unit vector $\mathbf{e}_n$. Setting up this device requires to create arbitrary static electric and magnetic fields in the laboratory, consistent with Maxwell's equations. The procedure is made explicit in [12]. Once constructed, the apparatus will split an incoming beam of particles with spin s into $N = (2s+1)$ subbeams corresponding to the eigenvalues of $\hat{C}$. The working principle is equivalent to that of a standard Stern-Gerlach apparatus where $\hat{C} \equiv \hat{S}_z$.

(*iv*) *Determination of the eigenvalues:* Prepare a spin s in a homogeneous mixture $\hat{\rho}_0 = \hat{I}/(2s+1)$. When carrying out measurements with the apparatus associated with $\hat{C}$, the output of each individual measurement will be one of the eigenvalues ζ_n of the matrix C. The actual values of the eigenvalues can be determined from the amount by which the particles in each subbeam are deflected from the straight line of flight. After sufficiently many repetitions, all eigenvalues ζ_n will be known. Since each eigenvalue occurs with probability $1/N$, the probability *not* to obtain one of the N values decreases exponentially with the number of runs.

By construction, the numbers ζ_n obtained in the last step coincide with the zeros of the polynomial $P(x)$, and one can write

$$P(x) = \prod_{n=1}^{N} (x - \zeta_n) \,. \tag{8}$$

The zeros ζ_n have been obtained by a genuinely quantum mechanical method.

Conclusions

It has been shown that one can build a quantum mechanical special-purpose machine which is capable to output the roots of a polynomial of degree N. The underlying working principle is to perform appropriate quantum mechanical measurements using a generalized Stern-Gerlach apparatus.

The possibility to extract information from individual quantum mechanical measurements may have implications for the interpretation of quantum mechanical states. Quantum root extraction of polynomials seems to strengthen the *individual* interpretation [13]: a single run of a measurement (with only one individual quantum system involved) provides information about one (randomly selected) zero of the polynomial; hence, no ensemble of identically prepared systems is required to obtain a useful answer from the experiment.

Instead of repeating the experiment $M \gg N$ times, one can imagine to run M identical experiments simultaneously, each generalized Stern-Gerlach apparatus being tuned to search for the zeros of the same polynomial $P(x)$. If the input state is an M-fold direct product of the homogeneous mixture $\hat{\rho}_0$,

$$\hat{\rho}_0 \otimes \ldots \otimes \hat{\rho}_0 \,, \tag{9}$$

the resulting 'parallel' quantum search would, with large probability, produce *all* zeros ζ_n at one go. In a sense, quantum mechanics is able to point almost instantaneously at the zeros of a given polynomial without any software program running.

Appendix: Modified Euclidean Algorithm

Given a polynomial

$$P(x) = x^N + p_{N-1}x^{N-1} + \ldots + p_0 \,, \quad p_n \in \mathsf{IR} \,, \tag{10}$$

the Modified Euclidean Algorithm [10] defines recursively a number of polynomials $P_k(x)$, $k = 2, 3, \ldots, N-1$, of smaller degrees, and it generates other polynomials $q_k(x)$ and numbers d_k which are required to define the hermitean companion matrix C. Start with

$$P_1(x) = P(x) \qquad P_2(x) = \frac{1}{N}\frac{dP(x)}{dx} \,, \tag{11}$$

and iterate the following steps. Divide $P_k(x)$ by $P_{k+1}(x)$,

$$P_k(x) = q_k(x)P_{k+1}(x) - r_k(x) \,, \tag{12}$$

with a remainder $r_k(x)$ which may either be different from or equal to zero. Denote by $d(Q(x))$ the coefficient of the highest power of the polynomial $Q(x)$: for example, $d(P(x)) = 1$. Define a polynomial $P_{k+2}(x)$ and the number d_k according to

$(\imath)$ $r_k(x) \neq 0 : P_{k+2}(x) = \frac{r_k(x)_k}{d_k}$ and $d_k = d(r_k(x))$;

$(\imath\imath)$ $r_k(x) = 0 : P_{k+2}(x) = \frac{dP_{k+1}(x)/dx}{d(dP_{k+1}(x)/dx)}$ and $d_k = 0$.

The algorithm terminates if $P_{k+1} = 1$, defining $q_k(x) = P_k(x)$. Otherwise the procedure is repeated with $P_{k+1}(x)$ and $P_{k+2}(x)$ in (11) and it will generate q_{k+1} and d_{k+1}, etc.

References

[1] P. W. Shor: *Algorithms for quantum computation: discrete log and factoring.* In: *Proceedings of the 35th Symposium on the Foundations of Computer Science*, edited by S. Goldwasser. IEEE Computer Society Press, 124 (1994) Los Alamitos

[2] M.A. Nielsen: *Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state.* quant-ph/0108020

[3] S.A. Fenner and Y. Zhang: *Universal quantum computation with two- and three-qubit projective measurements.* quant-ph/0111077

[4] D. W. Leung: *Two-qubit Projective measurements are Universal for Quantum Computation.* quant-ph/0111122v2

[5] L. Grover: Phys. Rev. Lett. **79** (1997) 325

[6] E. Farhi and S. Gutmann: Phys. Rev. A **57** (1998) 2403

[7] St. Weigert: J. Phys. A **34** (2001) 5619

[8] St. Weigert: Fortschr. Phys. **51** (2003) 248

[9] M. Fiedler: Linear Algebra Appl. **141** (1990) 265

[10] G. Schmeisser: Linear Algebra Appl. **193** (1993) 11

[11] R. Raussenberg and H.J. Briegel: Phys. Rev. Lett. **86** (2001) 5188

[12] A.R. Swift and R. Wright: J. Math. Phys. **21**, 77 (1977).

[13] M. Jammer: *Conceptual Foundations of Quantum Mechanics*, (Wiley, New-York 1974)