A quantum search for zeros of polynomials

Stefan Weigert

HuMP—Hull Mathematical Physics, Department of Mathematics,
University of Hull, Hull HU6 7RX, UK

E-mail: s.weigert@hull.ac.uk

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.

Keywords: Quantum algorithm, quantum measurements, hermitean
companion matrix

1. 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; see e.g. [1]. In [2], projective measurements have
been assigned a crucial role in a particular scheme of universal
quantum computation which requires measurements on up to
four qubits. Related schemes have been formulated based on
measurements on triples and pairs [3], and finally on pairs of
qubits only [4]. Measurements are also an essential part of
Grover's search algorithm—namely, in order to actually read
the result of the computation [5, 6].

A conceptually different strategy has been used in
proposing a special-purpose machine which is capable of
diagonalizing any finite-dimensional Hermitian matrix by
genuine quantum means, i.e. quantum measurements [7, 8].
In this approach of *quantum diagonalization*, a Hermitian
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.

2. The quantum search procedure

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

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

The assumption that $p_N = 1$ is not a restriction since
two polynomials $Q(x)$ and $Q(x)/c$, $c \neq 0$, have the same
zeros. The quantum procedure for identifying the zeros ζ_n
of $P(x)$ consists of two steps. First, one needs to find
a Hermitian 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 Hermitian matrix. Effectively,
they are obtained by measuring the eigenvalues of a quantum
mechanical spin observable $\hat{C}$ with matrix representation C.

3. The Hermitian companion matrix of a polynomial

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

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

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
μ_n, $n = 1, \ldots, N$, of the matrix M. Hermitian 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 *Hermitian* matrix C such that its characteristic polynomial is $P(x)$.

The matrix C is known as the *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 $C_U = UCU^\dagger$ provide solutions as well, where U is any unitary $(N \times N)$ matrix. The difficult part of the inverse problem lies in the requirement of finding a *Hermitian* matrix C: it is easy to specify a non-Hermitian companion matrix C_0 of the polynomial (1), namely,

$$C_0 = \begin{pmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ & & & 1 \\ -p_0 & -p_1 & \cdots & -p_{N-1} \end{pmatrix}. \quad (3)$$

Partial solutions of the problem of finding Hermitian companion matrices have been obtained in [9]. A complete and constructive solution can be found in [10], where a Hermitean 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

$$P(x) = (-)^N \det(C - xE), \quad (4)$$

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

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

The non-negative 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

(i) repeated division of polynomials;
(ii) evaluation of specific polynomials at $x = 0$;
(iii) taking square roots of positive numbers d_k.

As a corollary, the modified Euclidean algorithm checks whether the given polynomial has real zeros only: if any one of the numbers d_k is found to be negative, $P(x)$ cannot have real zeros only. For completeness, the algorithm is sketched in the appendix.

4. A quantum search for eigenvalues of Hermitian matrices

Four steps are necessary to find the eigenvalues of a given Hermitian matrix C with N different eigenvalues by means of quantum measurements. Here only an outline of this approach will be given; 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 (i) written in *standard form*; next, it is interpreted as (ii) a matrix representation of a unique *observable* $\hat{C}$ of a quantum spin; this observable can be measured by (iii) a specific *apparatus* which needs to be identified and built; finally, the apparatus is used to generate the eigenvalues by (iv) actually *measuring* the observable C.

(i) *The standard form of* C. Write the Hermitian $(N \times N)$ matrix C as a combination of linearly independent Hermitian *multipole* operators T_ν, $\nu = 0, \ldots, N^2 - 1$:

$$C = \sum_{\nu=0}^{N^2-1} c_\nu T_\nu, \qquad c_\nu = \frac{1}{N} \mathrm{Tr}[CT_\nu] \in \mathbb{R}. \quad (6)$$

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 Hermitian operators acting on an N-dimensional Hilbert space $\mathcal{H}$ [11]. These operators consist of all traceless symmetric products of up to N spin components $\hat{S} = (\hat{S}_x, \hat{S}_y, \hat{S}_y)$, plus the identity operator. Two multipoles are orthogonal with respect to a scalar product defined as the trace of their product: $(1/N) \mathrm{Tr}[\hat{T}_\nu \hat{T}_{\nu'}] = \delta_{\nu\nu'}$.

(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 $s = (N - 1)/2$:

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

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

(iii) *Setting up a measuring device for* $\hat{C}$. Swift and Wright have shown in [11] 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 $e_n \cdot \hat{S}$ along a direction specified by a unit vector e_n. Setting up this device requires one to create arbitrary static electric and magnetic fields in the laboratory, consistent with Maxwell's equations. The procedure is made explicit in [11]. 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 of *not* obtaining 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

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

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

5. Conclusions

It has been shown that one can build a quantum mechanical special-purpose machine which is capable of providing as output the roots of a polynomial of degree N. The underlying working principle is that of performing quantum mechanical measurements with a generalized Stern–Gerlach apparatus.

The present approach is genuinely different from existing quantum mechanical computations for finding the eigenvalues of a Hermitian operator, $\hat{H}$, say. This is typically done by means of *quantum phase estimation* in which the eigenphases of the unitary operator $\hat{U} = \exp[\mathrm{i}\hat{H}]$ are determined by a quantum algorithm [12, 13]. The algorithms require the efficient implementation of the operator $\hat{U}$ and (some of) its powers, followed by an (inverse) quantum Fourier transformation. If one desires to obtain the value of a phase ϕ with n relevant bits and a probability of success not smaller than $(1-\varepsilon)$, one needs to let the algorithms run for a time $\mathcal{O}(t^2)$ where $t = \ln[2+1/(2\varepsilon)]$ [14]. Furthermore, it has been argued in [15] that one can design a quantum algorithm to determine eigenvalues of specific ('exponentially large') Hamiltonians which runs in polynomial time while the best known classical algorithms require an exponential amount of time.

One could perform the matrix diagonalization required in the procedure to locate the zeros of a polynomial by each of the approaches just mentioned. Therefore, the question of the computational efficiency of the proposed special-purpose machine poses itself naturally, but it remains open for the time being.

The possibility of extracting information from *individual* quantum mechanical measurements in the present setting may have implications for the interpretation of quantum mechanical states. Quantum root extraction of polynomials seems to strengthen the *individual* interpretation [16]: 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 running 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 $\hat{\rho}_0$,

$$\hat{\rho}_0 \otimes \cdots \otimes \hat{\rho}_0, \qquad (9)$$

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. The modified Euclidean algorithm

Given a polynomial

$$P(x) = x^N + p_{N-1}x^{N-1} + \cdots + p_0, \qquad p_n \in \mathbb{R}, \qquad (10)$$

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 Hermitian companion matrix C. Start with

$$P_1(x) = P(x) \qquad P_2(x) = \frac{1}{N}\frac{\mathrm{d}P(x)}{\mathrm{d}x}, \qquad (11)$$

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

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

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

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

(ii) $r_k(x) = 0$: $P_{k+2}(x) = \frac{\mathrm{d}P_{k+1}(x)/\mathrm{d}x}{d(\mathrm{d}P_{k+1}(x)/\mathrm{d}x)}$ 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] Shor P W 1994 Algorithms for quantum computation: discrete log and factoring *Proc. 35th Symp. on the Foundations of Computer Science* ed S Goldwasser (Los Alamitos, CA: IEEE Computer Society Press) p 124
[2] Nielsen M A 2001 Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state *Preprint* quant-ph/0108020
[3] Fenner S A and Zhang Y 2001 Universal quantum computation with two- and three-qubit projective measurements *Preprint* quant-ph/0111077
[4] Leung D W 2001 Two-qubit projective measurements are universal for quantum computation *Preprint* quant-ph/0111122v2
[5] Grover L 1997 *Phys. Rev. Lett.* **79** 325
[6] Farhi E and Gutmann S 1998 *Phys. Rev.* A **57** 2403
[7] Weigert St 2001 *J. Phys. A: Math. Gen.* **34** 5619
[8] Weigert St 2003 *Fortschr. Phys.* **51** 248
[9] Fiedler M 1990 *Linear Algebra Appl.* **141** 265
[10] Schmeisser G 1993 *Linear Algebra Appl.* **193** 11
[11] Swift A R and Wright R 1977 *J. Math. Phys.* **21** 77
[12] Kitaev A Yu 1995 Quantum measurements and the Abelian stabilizer problem *Preprint* quant-ph/9511026
[13] Cleve R, Ekert A, Macchiavello C and Mosca M 1998 *Proc. R. Soc.* A **454** 339
[14] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[15] Abrams D S and Lloyd S 1999 *Phys. Rev. Lett.* **83** 5162
[16] Jammer M 1974 *Conceptual Foundations of Quantum Mechanics* (New York: Wiley)