On zeros of exponential polynomials and quantum algorithms

Yoshitaka Sasaki

Received: 27 August 2009 / Accepted: 7 October 2009 / Published online: 22 October 2009
© Springer Science+Business Media, LLC 2009

Abstract We calculate the zeros of an exponential polynomial of some variables by a classical algorithm and quantum algorithms which are based on the method of van Dam and Shparlinski, they treated the case of two variables, and compare with the time complexity of those cases. Further we consider the ratio (classical/quantum) of the exponent in the time complexity. Then we can observe the ratio is virtually 2 when the number of the variables is sufficiently large.

Keywords Quantum computing · Exponential congruence · Discrete logarithm · Character sum

PACS 02.10.De · 03.67.Lx

1 Introduction

Let $p$ be a prime number and let $\mathbb{F}_q$ denote a finite field with $q = p^\nu$ elements. $\mathbb{F}_q$ forms an additive group and $\mathbb{F}_q^\times := \mathbb{F}_q \setminus \{0\}$ forms a multiplicative group, where 0 is the zero element in $\mathbb{F}_q$. Any element of $\alpha \in \mathbb{F}_q^\times$ have a periodicity, that is there exists a smallest natural number $s$ such that $\alpha^s = 1$. We call such $s$ the “multiplicative order” of $\alpha$. It is known that the multiplicative order is a divisor of $\#\mathbb{F}_q^\times = q - 1$. See [5] for the details.

To evaluate the number of zeros of a homogeneous polynomial

$$F(x_0, \ldots, x_m) = \sum_{(n_0, \ldots, n_m) \in \mathbb{N}_0^{m+1}} a_{n_0, \ldots, n_m} x_0^{n_0} \cdots x_m^{n_m}$$

Y. Sasaki (✉)
Interdisciplinary Graduate School of Science and Engineering, Kinki University, Higashi-Osaka, Osaka 577-8502, Japan
E-mail: sasaki@alice.math.kindai.ac.jp
is a very important problem in mathematics. Here, $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ and $a_{n_1, \ldots, n_m} \in \mathbb{F}_q$. The zeta-function associated with such polynomial (the congruence zeta-function) was introduced to treat this problem. Particularly, the zeros of the congruence zeta-function satisfies an analogue of the Riemann hypothesis called “Weil conjecture”. Therefore, to investigate the zeros of the congruence zeta-function is very important. In [8], van Dam studied the zeros of the zeta-function associated with the Fermat surface by using quantum computing.

In [9], van Dam and Shparlinski treated the following exponential polynomial

$$f(x, y) = a_1 g_1^x + a_2 g_2^y - b$$

and calculated the zeros of (1.1) by quantum algorithms. Further they compared the time complexity of a classical algorithm with that of a quantum algorithm. Then the “cubic” speed-up was observed.

In this article, we treat the exponential polynomial of $n$ variables

$$f_b(x_1, \ldots, x_n) := a_1 g_1^{x_1} + \cdots + a_n g_n^{x_n} - b,$$

where $a_i, g_i \in \mathbb{F}_q^\times (i = 1, \ldots, n)$ and $b \in \mathbb{F}_q$. We restrict $n \ll q^\varepsilon$ for a small $\varepsilon > 0$, where $A \ll B$ means $A = O(B)$. The reason why we claim this restriction will be explained in Appendix, below. We calculate the solutions of $f_b(x_1, \ldots, x_n) = 0$ by using quantum algorithms which are natural generalizations of the method of van Dam and Shparlinski. Further we also compare the time complexity of a classical algorithm with that of a quantum algorithm. Then a reduction in the exponent by a factor of $(2n - 1)/(n - 1)$ is observed. We notice that $(2n - 1)/(n - 1) = 2 + 1/(n - 1)$ is virtually 2 when $n$ is sufficiently large. This is the boundary between a classical algorithm and our quantum algorithm. In the previous report [6], Ohno, Sasaki and Yamazaki treated the case of three variables and obtained the ratio $5/2$.

In the next section, we introduce some notation and give the considerable lemma which supports whether there exist solutions of (1.2). In Sect. 3, we calculate the time complexity of a classical algorithm. Further in Sect. 4, we calculate the time complexity of a quantum algorithm.

2 The number of solution of equation

In this section, we describe an important formula which expresses the density of solutions of

$$f_b(x_1, \ldots, x_n) = 0$$

as Lemma 2.1, below. Lemma 2.1 is often used in the following sections. To state it, we introduce some notation.