Using Grover's Algorithm for finding Multiplication Algorithms on finite fields

Yigit Yargic

January 13, 2023

We consider the following task: Given the indeterminates $\{a_k\}_{k=1,\ldots,D_a}$ and $\{b_l\}_{l=1,\ldots,D_b}$, we want to compute the bilinear expressions $\{c_j\}_{j=1,\ldots,D_c}$ defined as

$$c_j = \sum_{k,l} C_{jkl}\, a_k b_l \tag{1}$$

for some fixed 3-tensor C_{jkl}, while doing at most M multiplications between $\{a_k\}$ and $\{b_l\}$. This task is equivalent to solving the tensor rank decomposition

$$C_{jkl} = \sum_{\mu=1}^{M} \gamma_{j,\mu}\, \alpha_{k,\mu}\, \beta_{l,\mu} \tag{2}$$

for the parameters $\{\alpha_{k,\mu}\}$, $\{\beta_{l,\mu}\}$, and $\{\gamma_{j,\mu}\}$.

We further restrict our attention here to a finite field $\mathbb{F}_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime power. All indeterminates, parameters, and the entries of C_{jkl} are taken on $\mathbb{F}_{\mathfrak{p}}$.

We write the parameters as $x = (\alpha_{k,\mu}, \beta_{l,\mu}, \gamma_{j,\mu}) \in \{0, \ldots, \mathfrak{p}-1\}^{M(D_a+D_b+D_c)}$ in a compact notation. We introduce the function

$$f(x) = \begin{cases} 1\,, & \text{if } x = (\alpha_{k,\mu}, \beta_{l,\mu}, \gamma_{j,\mu}) \text{ solves (2)}, \\ 0\,, & \text{otherwise.} \end{cases} \tag{3}$$

In a direct, classical search, there are $Q \equiv \mathfrak{p}^{M(D_a+D_b+D_c)}$ different values of x to try. Let's say there are q different values of x which satisfy $f(x) = 1$, and $0 < q \ll Q$. The expected time for this search to find an instance of $f(x) = 1$ will be $\tau \equiv Q/q$.

With a *quantum* algorithm, we can get quadratic improvement in the expected time of this search for a multiplication algorithm. Let's represent the variable $x \in \{0, \ldots, Q-1\}$ as a Q-level qudit $|x\rangle$. Our aim is to start from the quantum state

$$|\psi_0\rangle = \frac{1}{\sqrt{Q}} \sum_x |x\rangle \ , \tag{4}$$

where we have a uniform probability for measuring each x, and then use unitary operators to turn this into another state where we will have a higher probability of measuring an eigenvalue x with $f(x) = 1$. ("Grover's amplitude amplification")

We introduce two unitary operators (in fact, reflections). The first one is

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle \ . \tag{5}$$

The second one is

$$U_G = 2 |\psi_0\rangle\langle\psi_0| - \mathbb{1} \ . \tag{6}$$

We will iteratively apply the composite operator $U_G U_f$ on $|\psi_0\rangle$ for r iterations, and get a more favorable state. Let's discuss how this works and what r is.

Consider the two orthogonal states

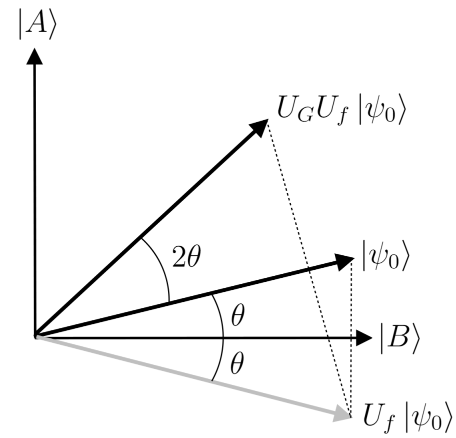
$$|A\rangle = \frac{1}{\sqrt{q}} \sum_{x:f(x)=1} |x\rangle \qquad \text{and} \qquad |B\rangle = \frac{1}{\sqrt{Q-q}} \sum_{x:f(x)=0} |x\rangle \ . \tag{7}$$

The state $|\psi_0\rangle$ lies on the 2-dimensional plane spanned by $|A\rangle$ and $|B\rangle$,

$$|\psi_0\rangle = \sin\theta \, |A\rangle + \cos\theta \, |B\rangle \ , \qquad \sin\theta = \sqrt{\frac{q}{Q}} = \tau^{-1/2} \ . \tag{8}$$

The operator U_f is a reflection through $|B\rangle$, while the operator U_G is a reflection through $|\psi_0\rangle$. Hence,

$$\begin{aligned}
|\psi_0\rangle &= \cos\theta \, |B\rangle + \sin\theta \, |A\rangle \ , \\
|\psi_0'\rangle = U_f \, |\psi_0\rangle &= \cos\theta \, |B\rangle - \sin\theta \, |A\rangle \ , \\
|\psi_1\rangle = U_G \, |\psi_0'\rangle &= \cos(3\theta) \, |B\rangle + \sin(3\theta) \, |A\rangle \ , \\
|\psi_1'\rangle = U_f \, |\psi_1\rangle &= \cos(3\theta) \, |B\rangle - \sin(3\theta) \, |A\rangle \ , \\
|\psi_2\rangle = U_G \, |\psi_1'\rangle &= \cos(5\theta) \, |B\rangle + \sin(5\theta) \, |A\rangle \ , \\
&\cdots
\end{aligned} \tag{9}$$



or generally,

$$|\psi_r\rangle = U_G U_f |\psi_{r-1}\rangle = \cos((2r+1)\theta)|B\rangle + \sin((2r+1)\theta)|A\rangle \ . \tag{10}$$

We want to find $r \in \mathbb{N}$ such that

$$(2r+1)\theta \approx \frac{\pi}{2} \ . \tag{11}$$

In other words,

$$r \approx \frac{1}{2}\left(-1 + \frac{\pi}{2\arcsin(\tau^{-1/2})}\right) \underset{\tau\to\infty}{\approx} \frac{\pi}{4}\sqrt{\tau} \ . \tag{12}$$

After $r \approx \frac{\pi}{4}\sqrt{\tau}$ iterations of applying the unitary operator $U_G U_f$ on the initial quantum state $|\psi_0\rangle$, we will create a state $|\psi_r\rangle$ such that

$$\angle(|\psi_r\rangle, |A\rangle) \leq \theta \ . \tag{13}$$

Therefore, when we measure $|\psi_r\rangle$, there will be at least a chance of $\cos^2(\theta) = 1 - \frac{1}{\tau}$ to measure an instance of x such that $f(x) = 1$.

Considering that we only had to apply the function f in this quantum algorithm $\frac{\pi}{4}\sqrt{\tau}$ times, compared to τ times in the classical algorithm, a quantum computer would reduce the time for finding optimal multiplication algorithms quadratically.