Quantum Computing: Example Sheets 3 and 4

1. For n-bit strings $x = x_1 \dots x_n$ and $a = a_1 \dots a_n$ in B_n, we have the sum $x \oplus a$ which is an n-bit string and now introduce the 1-bit "dot product":

$$x \cdot a = x_1 a_1 \oplus x_2 a_2 \oplus \dots \oplus x_n a_n \ .$$

For any fixed n-bit string $a = a_1 \dots a_n$, consider the function $f_a : B_n \to B_1$ given by

$$f_a(x_1, \dots, x_n) = x \cdot a$$

(i) Show that for any $a \neq 00\dots0$, f_a is a balanced function (i.e., f_a has value 0 on exactly half the inputs x, and value 1 on the other half).

(ii) Given a classical black box that computes f_a, describe a classical deterministic algorithm that will identify $a = a_1 \dots a_n$ on which f_a is based. Show that any such classical algorithm has query complexity at least n.

Now define $H_n = H \otimes \dots \otimes H$ as the application of Hadamard H to each qubit in a row of n. Show that for $x \in B$ and $a \in B_n$,

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{xy} |y\rangle, \quad H_n|a\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in B_n} (-1)^{a \cdot y} |y\rangle$$

(iii) (The Bernstein-Vazirani algorithm.) For each a, consider the function f_a which is a balanced function if $a \neq 00\dots0$. Show that the Deutsch-Jozsa algorithm will perfectly distinguish and identify the $2^n - 1$ balanced functions f_a (for $a \neq 00\dots0$) with only *one* query to the quantum oracle for f. Show that the n-bit output gives the string a with certainty for these special balanced functions.

2. Exponentiation of integers mod N is a basic arithmetic task. (It will be used for example in Shor's algorithm), and it is important to know that it can be done in polynomial time poly(n), where $n = \log N$ is the number of digits for integers in $\mathbb{Z}_N$.

To compute, say, 3^k mod N (for $k \in \mathbb{Z}_N$ and $N > 3$), we could multiply 3 together k times. Show that this is not a poly(n)-time computation.

Devise an algorithm that does run in poly(n) time. [*Hint: consider repeated squaring.*]

You may assume that multiplication of integers in $\mathbb{Z}_N$ can be done in $O(n^2)$ time. Generalise to a polynomial-time computation of $k_1^{k_2} \bmod N$ for $k_1, k_2 \in \mathbb{Z}_N$, showing that it may be computed in $O(n^3)$ time.

3. Simon's decision problem is the following:

Input: An oracle for a function $f : B_n \to B_n$,

Promise: f is either (a) a one-to-one function, or (b) a two-to-one function of the following special form: there exists $\xi \in B_n$ such that $f(x) = f(y)$ iff $y = x \oplus \xi$ ((i.e. ξ is the period of f when its domain is viewed as the group $(\mathbb{Z}_2)^n$).

Problem: Determine whether (a) or (b) applies, with success probability at least $1 - \varepsilon$ for any $\varepsilon > 0$.

It can be argued that, for classical computation, this requires at least $O(2^{n/4})$ queries to the oracle. The goal of this question is to develop a quantum algorithm that solves the problem with quantum query complexity only $O(n)$. Even more, the algorithm will determine the period ξ if (b) holds. Thus (unlike the balanced vs. constant problem), we'll have a provable exponential separation between classical and quantum query complexities, even in the presence of bounded error.

To begin, consider $2n$ qubits: the first n comprising the input register, and the last n comprising the output register for a quantum oracle U_f computing f, i.e.,

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

for n-string qubits x and y.

(i) Let all qubits start in state $|0\rangle$. Apply Hadamard $H^{\otimes n}$ to the input register, apply U_f, and then measure the output register (all measurements being in the computational basis).

Write down the generic form of the n-qubit state $|\alpha\rangle$ of the input register after the measurement. Suppose we then measure $|\alpha\rangle$. Would the result provide any information about the period ξ?

(ii) Having obtained $|\alpha\rangle$ above, apply $H^{\otimes n}$ to get a state denoted $|\beta\rangle$. Show that if we measure $|\beta\rangle$, then the n-bit outcome is a uniformly random string y satisfying $\xi \cdot y = 0$ (so any such y is obtained with probability $1/2^{n-1}$.)

Now we run this algorithm repeatedly, each time independently obtaining another string y satisfying $\xi \cdot y = 0$. Recall that $B_n = (\mathbb{Z}_2)^n$ is a vector space over the field $\mathbb{Z}_2$. If $y_1, \ldots, y_s$ are s linearly independent bit strings, then their linear span contains 2^s of the 2^n vectors in B^n. Furthermore, solving systems of linear equations over B_n can be done via Gaussian elimination in poly(n) time.

(iii) Show that if $n-1$ bit strings y_i are chosen uniformly at random and independently, satisfying $\xi \cdot y_i = 0$, then they will be linearly independent (and not include the all-zero string $00\ldots0$) with probability

$$\prod_{k=1}^{n-1}\left(1-\frac{2^{k-1}}{2^{n-1}}\right) = \frac{1}{2}\prod_{k=1}^{n-2}\left(1-\frac{2^{k-1}}{2^{n-1}}\right)$$

Show that this is at least $1/4$.
[Hint: Use the inequality $(1-a)(1-b) \geq 1-(a+b)$ *for* $a, b \in [0,1]$*.]*

(iv) Explain how this process may be used to solve Simon's problem with $O(n)$ quantum query complexity for any desired success probability $1-\varepsilon$.

4. Let B_n denote the set of all n-bit strings. The *Hamming distance* between two n-bit strings $a = a_1 \ldots a_n$ and $x = x_1 \ldots x_n$ is the number of places j where a_j and x_j differ. Let $H_a : B_n \to B_2$ be the function

$$H_a(x) = \text{Hamming distance between } a \text{ and } x) \bmod 4 \ .$$

Here we are identifying B_2 with $\mathbb{Z}_4$ via the usual binary representations of 0,1,2,3. (For example if $a = 101110000$ and $x = 001001110$ then $H_a(x) = 6 \bmod 4 = 2$.)

Now consider the promise problem *HAM-mod4*:

Input: A black-box function $f : B_n \to B_2$

Promise: $f = H_a$ for some N-bit string a.

Goal: Determine a with certainty

In the quantum context, the black box is a unitary operation on $n+2$ qubits given by:

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

Here the x register is n qubits, and in the y register we'll write the basis states $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ with additin in the expression $y + f(x)$ being addition in $\mathbb{Z}_4$.

(i) Show that classically, the query complexity of HAM-mod4 is at least $n/2$.

We will now show that the problem can be solved quantumly with just *one* query. Let M be the unitary matrix

$$M = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \ . \tag{1}$$

Introduce the 1-bit functions $h_0, h_1 : B_1 \to B_1$ where:

$$h_0(0) = 0, \quad h_0(1) = 1; \quad h_1(0) = 1, \quad h_1(1) = 0$$

i.e., h_a is just H_a for a 1-bit string a.

(ii) For $a_1 = 0$ or 1, show that

$$M|a_1\rangle = \frac{1}{\sqrt{2}} \sum_{x_1=0}^{1} i^{h_{a_1}(x_1)} |x_1\rangle$$

(iii) For n-bit strings $a = a_1 \dots a_n$ and $x = x_1 \dots x_n$, show that

$$H_a(x) = h_{a_1}(x_1) + \cdots + h_{a_n}(x_n) \mod 4$$

Hence, describe how to prepare the state

$$|H_a\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} i^{H_a(x)} |x\rangle$$

starting from $|a\rangle$.

(iv) Let S denote the 2-qubit "shift" operation

$$S|y\rangle = |y + 1 \mod 4\rangle, \quad y \in \mathbb{Z}_4$$

Let QFT denote the quantum Fourier transform mod 4. Calculate $|\psi_3\rangle = QFT|3\rangle$ and show $S|\psi_3\rangle = i|\psi_3\rangle$.

(v) Use the above results to design a quantum algorithm that solves HAM-mod4 with certainty using just one query to U_f and poly(n) total time complexity. [*Hint: it may be useful to note that* $U_{H_a}|x\rangle|y\rangle = |x\rangle S^{H_a(x)}|y\rangle$. Draw a circuit diagram to represent your quantum algorithm.

Comment: This algorithm is structurally similar to the Bernstein–Vazirani algorithm. Compare the corresponding ingredients and their functionality. What corresponds to QFT, $|\psi_3\rangle$, M, h_a, and H_a?

5a. Let U_1, V_1, U_2, V_2 be unitary gates. Show that if $\|U_1 - V_1\| \leq \varepsilon_1$ and $\|U_2 - V_2\| \leq \varepsilon_2$ (i.e. the V's are "approximate versions" of the U's), then

$$\|U_2 U_1 - V_2 V_1\| \leq \varepsilon_1 + \varepsilon_2 \ .$$

That is, errors in using approximate versions at most add when gates are composed. (Recall that $\|U - V\|$ is defined as the maximum length of the vector $(U - V)|\psi\rangle$ over all normalised $|\psi\rangle$.)

Deduce that if $\|U_i - V_i\| \leq \varepsilon$ for $i = 1, \ldots, n$, then $U_n \cdots U_1 - V_n \cdots V_1\| \leq n\varepsilon$.

b. For the purposes of this question, assume the following: if a gate set is approximately universal, then any one- or two-qubit gate U may be approximated to within ε by a circuit composed of gates from the set, with size poly$(1/\varepsilon)$. (In fact, the Solovay–Kitaev theorem says even poly$(\log(1/\varepsilon))$ gates suffice, but you do not need this here.)

Let G and H be two approximately universal gate sets, each consisting of one- and two-qubit gates. Suppose a decision problem D is in the class **BQP** with all gates from the set G. Show that D is also in **BQP** when using only gates from the set H. (That is, the definition of **BQP** does not depend on the particular approximately universal gate set used.)

6. Consider the function $f(x) = 5^x \bmod 39$. on the domain $x \in \mathbb{Z}_{2^m}$ with $m = 11$.

(i) Show that f is periodic, and determine its period r. (You may need a calculator!)

(ii) Suppose we construct the equal superposition state over pairs $|f\rangle$ of $(x, f(x))$ values over the domain $\mathbb{Z}_{2^m}$, measure the second register, perform the quantum Fourier transform mod 2^m on the post-measurement state of the first register, and finally measure it. What is the probability for each possible outcome $0 \leq c < 2^m$ in the final measurement? (Note: this should require very little calculation!)

What is the probability that we successfully determine the period r from this measurement result, using the standard process of the quantum period-finding algorithm?

7. Consider a quantum computation given by a family of polynomial-size quantum circuits $\{C_1, C_2, \ldots, C_n, \ldots\}$ where each C_n comprises gates from a universal set G consisting of only one- and two-qubit gates. Suppose this quantum computation solves a decision problem A in **BQP**.

Further, assume that for any input $x \in B_n$ to the circuit C_n (for any n), the quantum state remains unentangled at every stage of the computation – that is, the state is

always a product state over all the qubits involved. Show that in this case, the problem A is also in **BPP**. (That is, if no entanglement is ever present in a quantum computation, then it cannot provide any computational benefit over classical computation beyond at most a polynomial overhead in time). [*Hint: Consider simulating the entire quantum process step-by-step on a classical computer.*]

8. For the plane $P(x_0)$ spanned by $|x_0\rangle$ and $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B_n} |x\rangle$. set up an orthonormal basis in the plane. Then, using this basis, show algebraically (rather than geometrically as in lectures) that the Grover iteration operator Q is a rotation in the plane, and derive the angle of rotation.

9. Consider Grover's algorithm for a unique good item x_0 in a search space of size $N = 2^n$. Suppose that instead of the usual uniform superposition state $|\psi_0\rangle$, we start with an arbitrary state $|\eta_0\rangle$ of n qubits and conduct the algorithm just as before – i.e., apply $\left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ iterations of Q and measure.

When $|\eta_0\rangle = |\psi_0\rangle$, the final measurement yields x_0 with probability 1, up to terms of order $1/N$. If instead we begin with some other starting state $|\eta_0\rangle$, describe geometrically how $|\eta_0\rangle$ evolves during the computation. Give an expression (up to terms of order $1/N$) for the probability of obtaining x_0 in the final measurement. Show that this probability may generally be improved by changing the number of Grover iterations.

10a. Consider the operator $-I_{|\psi_0\rangle} = 2|\psi_0\rangle\langle\psi_0| - I$, where $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B_n} |x\rangle, \quad N = 2^n$. Show that:

$$-I_{|\psi_0\rangle} = \frac{2}{N} \sum_{x,y} |x\rangle\langle y| - I.$$

b. Let $|\alpha\rangle = \sum_x a_x |x\rangle$ be any n-qubit state. Define the average amplitude as $\bar{a} = \frac{1}{N} \sum_x a_x$. Define the operation R of *inversion in the average* as follows: $R|\alpha\rangle = \sum_x a'_x |x\rangle$ where $a'_x = a_x - 2(a_x - \bar{a})$. Using the formula in part (a), show that $-I_{|\psi_0\rangle}|\alpha\rangle = R|\alpha\rangle$.

c. Hence, Grover's algorithm may be described as follows: start with the state $|\psi_0\rangle$; then flip the sign of the x_0 amplitude; then apply R, the inversion about the average; then Iterate the last two steps alternately.

Represent states with real amplitudes as a graph where the x-axis labels basis states x, and the amplitude for each state is drawn as a (positive or negative) vertical bar. Using this pictorial representation, starting with $|\psi_0\rangle$, carry out one or two iterations of the "flip x_0 and then do R" operation to observe how the initial amplitude distribution, uniform over all x, begins to concentrate on x_0.

d. Consider the definite case of $N = 4$ (i.e. $x \in \{0, 1, 2, 3\}$), and take $x_0 = 3$. Draw the pictorial graph representation of $|\psi_0\rangle$ and carry out one Grover iteration as a flip followed by inversion in the average. Show that as a result, the amplitude becomes exactly zero at $x \neq x_0$ and 1 at $x = x_0$.

11. For any prime p, consider the set $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} \subset \mathbb{Z}_p$ of nonzero integers modulo p, with multiplication modulo p as the group operation. A *generator* g for $\mathbb{Z}_p^*$ is an element such that its powers generate all of $\mathbb{Z}_p^*$, i.e. for every $x \in \mathbb{Z}_p^*$, there exists $y \in \mathbb{Z}_{p-1}$ such that $x = g^y \bmod p$. This y is called the *discrete logarithm* of x to the base g.

Assume that $\mathbb{Z}_p^*$ always has a generator g, and that $g^{p-1} \equiv 1 \bmod p$. Suppose we are given a generator g and an element $x \in \mathbb{Z}_p$, and we wish to compute its discrete logarithm y

(i) Consider the function $f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ defined by:

$$f(a, b) = g^a x^{-b} \bmod p.$$

Show that for each fixed $c \in \mathbb{Z}_p^*$, there exists a fixed $k \in \mathbb{Z}_{p-1}$ such that

$$f(a, b) = c \iff a = by + k \bmod (p-1).$$

(ii) Suppose we prepare the quantum state

$$|\varphi\rangle = \frac{1}{p-1} \sum_{a,b \in \mathbb{Z}_{p-1}} |a\rangle|b\rangle|f(a, b)\rangle$$

in the Hilbert space $\mathcal{H}_{p-1} \otimes \mathcal{H}_{p-1} \otimes \mathcal{H}_p$, where $\mathcal{H}_n$ denotes a space of dimension n with orthonormal basis $\{|k\rangle : k \in \mathbb{Z}_n\}$. Measure the third register and obtain some value c_0. Determine the post-measurement state of the first two registers.

(iii) Apply the quantum Fourier transform mod $(p-1)$ to both of the first two registers and then measure them. Which output pairs $(c_1, c_2) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ can be obtained with non-zero probability?

Can y be determined from any such pair?

Hence, outline a quantum algorithm for computing discrete logarithms that runs in time $O(\text{poly}(\log p))$ for large p and succeeds with probability at least $1 - \varepsilon$, for any constant $\varepsilon > 0$. [*You may assume that both f and the quantum Fourier transform mod $p - 1$ can be implemented in $O(\text{poly}(\log p))$ time.*]

12. We wish to factor $N = 21$ using Shor's algorithm, and we have chosen $a = 2$ so that we aim to determine the period of the function $f(x) = 2^x \bmod 21$. We proceed through the quantum part of the algorithm and finally measure the x-register. Suppose we obtain measurement result $c = 427$.

(i) What is the number m of qubits used for the x-register?

(ii) Use the continued fraction method to find a fraction j/r with denominator less than 21 that is within $1/2^{m+1}$ of the ration $c/2^m$.

(iii) We hope that the denominator r of j/r (when the fraction is in lowest terms) is the period of $f(x)$. Check whether this is indeed the case in this example. Then, using your value of r, complete the classical post-processing to find nontrivial factors of 21 following the standard method used in Shor's algorithm.

13a. Let $N = 2^n$, and let $f : B_n \to B_1$ be a function that takes the value 1 exactly K times, with $f(x) = 1$ iff $x \in G = \{x_1, \ldots, x_K\}$. The Grover operator is defined as: $Q = -H_n I_0 H_n I_G$, where $H_n = H^{\otimes n}$ is the Hadamard transform on n qubits and, for all $x \in B_n$, the phase inversion operators I_0 and I_G are defined by:

$$I_0|x\rangle = \begin{cases} -|x\rangle & \text{if } x = 00\ldots0 \\ |x\rangle & \text{otherwise} \end{cases} \quad \text{and} \quad I_G|x\rangle = \begin{cases} -|x\rangle & \text{if } x \in G \\ |x\rangle & \text{otherwise} \end{cases}$$

Let $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B_n} |x\rangle$ and $|\psi_G\rangle = \frac{1}{\sqrt{K}} \sum_{x \in G} |x\rangle$. Derive a geometric interpretation of the action of Q in the 2d subspace of the n-qubit Hilbert space spanned by $|\psi_0\rangle$ and $|\psi_G\rangle$.

Using this interpretation, show that if I_G is given as a black box, then an $x \in G$ may be found with high probability (say, greater than 1/2) using $O(\sqrt{N/K})$ applications of I_G, assuming N is large and $K \ll N$.

b. Let $g : B_n \to B_n$ be a 2-to-1 function: for every y in the range of g, there exist exactly two strings $x \in B_n$ such that $g(x) = y$. A *collision* is a pair of strings $x_1, x_2 \in B_n$ such that $g(x_1) = g(x_2)$. The standard quantum oracle U_g for g is defined on $2n$ qubits by

$$U_g|x\rangle|y\rangle = |x\rangle|y \oplus g(x)\rangle \quad x, y \in B_n,$$

where $\oplus$ denotes bitwise addition of n-bit strings.

Suppose that we are given U_g as a black-box operation. Using the result of (a), or otherwise, show that a collision may be found with high probability (say, greater than 1/2) using $O(N^{1/3})$ queries to U_g. [*Hint: Start by partitioning the domain of g into*

two sets A and B of sizes $N^{1/3}$ and $N - N^{1/3}$ respectively. List all values of $g(x)$ for $x \in A$. If a collision is not found there, what should we do next with B?]

Comment: The classical query complexity for collision finding is $O(\sqrt{N})$. The $O(N^{1/3})$ upper bound on quantum query complexity shown here is known to be optimal.

14a. For the state space $\mathcal{H}_N$ with orthonormal basis $\{|k\rangle : k \in \mathbb{Z}_N\}$, consider the unitary *shift operator* S defined by $S|k\rangle = |k+1 \bmod N\rangle$ for all $k \in \mathbb{Z}_N$. Also define the states: $|\chi_k\rangle = QFT_N|k\rangle$ called *shift-invariant states*.

Show that each $|\chi_k\rangle$ is an eigenstate of S, and determine the corresponding eigenvalue.

Let $|\psi\rangle$ be any state in $\mathcal{H}_N$. Show that for any $m \in \mathbb{Z}_N$, the outcome probabilities of measuring $S^m|\psi\rangle$ in the $\{|\chi_k\rangle\}$ basis are independent of the shift m. (This gives an alternative explanation for the efficacy of the QFT in the period-finding algorithm.)

b. Let x, N be two positive integers with $x < N$. Define the operator U_x on $\mathcal{H}_N$ by: $U_x|y\rangle = |xy \bmod N\rangle$ for all $y \in \mathbb{Z}_N$.

(i) Show that U_x is unitary if and only if x and N are coprime.

Assume now that x and N are coprime. Let r be the *order* of x mod N, i.e. the smallest $t > 0$ such that $x^t \equiv 1 \bmod N$. For $0 \le s \le r-1$, define:

$$|\psi_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} |x^k \bmod N\rangle.$$

(ii) Show that each state $|\psi_s\rangle$ is an eigenvector of U_x with eigenvalue $e^{2\pi i s/r}$.

(iii) Show that $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_s\rangle = |1\rangle$.

c. Suppose we have a quantum process $\mathcal{A}$ with the following property: for any unitary V, and for any eigenstate $|\xi_\lambda\rangle$ of V with eigenvalue $e^{2\pi i\lambda}$, the process $\mathcal{A}$ is a unitary operation such that $\mathcal{A}(|\xi_\lambda\rangle \otimes |0\rangle) = |\xi_\lambda\rangle \otimes |\lambda\rangle$ where the second register (initially $|0\rangle$) is of suitable size to hold the value λ (we ignore precision issues here). This process is known as the *phase estimation algorithm*. Assume that $\mathcal{A}$ is available for the case $V = U_x$, and that in this case it runs in poly$(\log N)$ time (which is true).

Show how the results of (b) together with the phase estimation algorithm for $V = U_x$ can be used to provide a poly$(\log N)$-time quantum algorithm for factoring N (called

Kitaev's factoring algorithm). [*Hint: start with the reduction of factoring to order finding, as done in Shor's algorithm.*]

15. Let $\mathbf{x} = x_0 x_1 \ldots x_{N-1}$ be an N-bit string. We can think of $\mathbf{x}$ as specifying the values of a function from $\mathbb{Z}_N$ to $\{0,1\}$. A quantum oracle $O_\mathbf{x}$ for $\mathbf{x}$ is a unitary operator acting on a state space of dimension $2N$, defined by $O_x|i\rangle|y\rangle = |i\rangle|y \oplus x_i\rangle$ for $i \in \mathbb{Z}_N$ and $y \in \{0,1\}$ where $\oplus$ denotes addition modulo 2. [Note: This generalises the notion of an oracle for $f : B_n \to B_1$, corresponding to domain size $N = 2^n$, to arbitrary domain sizes not necessarily powers of 2.]

Consider the following oracle problem *BAL*

Input: Oracle $O_\mathbf{x}$ for some N-bit string $\mathbf{x}$, where $N = 2^K$ is even.

Goal: Decide with certainty whether $\mathbf{x}$ is (i) balanced or (ii) not balanced. (Here "balanced" means that exactly half of the bits are 0, half are 1).

We know that with the promise that $\mathbf{x}$ is either balanced or constant, the Deutsch–Jozsa algorithm solves the problem with just one query. However, in the absence of such a promise, it can be shown that any quantum algorithm solving the problem requires at least $\Omega(N^{1/6})$ queries (i.e. exponential in n when $N = 2^n$). The exact optimal quantum query complexity is not known.

(a) Show that any classical deterministic algorithm that solves problem BAL for all possible inputs must make at least $N = 2K$ queries to the oracle in the worst case.

We now develop a quantum algorithm that solves BAL with at most $K = N/2$ queries, thus improving (modestly) on any classical algorithm.

(b) Begin by writing $\hat{x}_i = (-1)^{x_i}$, and work in a state space of dimension N^2 with orthonormal basis states $|i\rangle|j\rangle$ for $i, j \in \mathbb{Z}_N$. Consider the following three computational steps:

- **Step 1:** Prepare the state $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle|0\rangle$ and, together with a qubit state in $|-\rangle$, use one query of the oracle to produce

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \hat{x}_i |i\rangle|0\rangle.$$

- **Step 2:** Define a transformation U whose action on states $|i\rangle|0\rangle$ is

$$U : |i\rangle|0\rangle \mapsto \frac{1}{\sqrt{N}} \left(\sum_{k>i} |i\rangle|k\rangle - \sum_{k<i} |k\rangle|i\rangle + |0\rangle|0\rangle \right).$$

By linearity, the state after applying U to $|\psi_1\rangle$ becomes

$$|\psi_2\rangle = U|\psi_1\rangle = \left(\frac{1}{N}\sum_{i=0}^{N-1}\hat{x}_i\right)|0\rangle|0\rangle + \sum_{i<j}\frac{\hat{x}_i - \hat{x}_j}{N}|i\rangle|j\rangle.$$

- **Step 3:** Measure $|\psi_2\rangle$ in the standard basis to obtain an outcome (k, ℓ) with $k, \ell \in \mathbb{Z}_N$.

(i) Show that there exists a unitary transformation $\widetilde{U}$ acting on the full state space whose action on states $|i\rangle|0\rangle$ agrees with U.

(ii) Suppose we now impose a promise that $\mathbf{x}$ is either balanced or constant. What can we conclude from seeing $(0, 0)$ or some $(i, j) \neq (0, 0)$ as the measurement outcome?

(iii) Now return to the general case. Considering the possible measurement outcomes (k, l), show that problem BAL may still be solved with certainty using at most $K = N/2$ queries to the oracle, by repeating or adapting the steps above appropriately.