

Cryptography Assignment 5

The conjugate of a complex number $a + bi$ is $x^* = a - bi$. For a matrix U with complexity entries u_{ij} , U^* is the matrix with entries u_{ij}^* . A matrix U is unitary if $U(U^*)^T = I$ where $(U^*)^T$ is the transpose of U^* and I is the identity matrix. Quantum computing works only with unitary transformations.

1. Show that if $x = e^{iy}$ then $x^* = e^{-iy}$.
2. Show that the linear transformation given by Shor's algorithm is unitary (U is an $N \times N$ matrix and $u_{ij} = \frac{e^{2\pi ij/N}}{\sqrt{N}}$).
3. Consider a transformation that maps a vector $v = (v_1, \dots, v_n)$ to $(2\sigma - v_1, \dots, 2\sigma - v_n)$ where σ is the average of the v_i 's. Show that this transformation is linear and unitary. This is the main transformation used for Grover's algorithm.
4. In the Bennett-Brassard quantum key distribution we used angles $0^\circ, 45^\circ, 90^\circ$ and 135° . What goes wrong if instead we used angles $0^\circ, 10^\circ, 90^\circ$ and 100° ? Is there a variation of this protocol that would still work well with these angles?