The following problem asks you to understand the Grover's algorithm loop in a different way. Let $|\psi\rangle$ be the state that we're rotating. That is, $|\psi\rangle$ starts as $|\phi\rangle$ and then gradually approaches $|\omega\rangle$. Suppose that we're somewhere in the middle of this loop, and we're wondering whether we should rotate $|\psi\rangle$ another time. Well, we should rotate it as long as the inner product of $|\psi\rangle$ with $|\omega\rangle$ keeps increasing. So we ask ourselves: How does $\langle\omega| W \cdot f |\psi\rangle$ compare to $\langle\omega| |\psi\rangle$?

A. Using algebra, show that $\langle\omega| W \cdot f |\psi\rangle - \langle\omega| |\psi\rangle > 0$ if and only if $(\langle\phi| - 2^{1-n/2} \langle\omega|) |\psi\rangle > 0$. Then interpret the latter inequality geometrically.

The following problem is inspired by a true story. To understand it, you need to know the repeated squaring algorithm. Here's the short version. If you want to raise a quantity A (a number, matrix, function, whatever) to a high power k, then don't do it the naive way:

$$A^k = \underbrace{A \cdot A \cdot \cdots \cdot A}_{k \text{ times}}.$$

That approach uses about k multiplications. Instead, raise A to powers of 2 by repeatedly squaring A:

$$A^2 = A \cdot A, \quad A^4 = A^2 \cdot A^2, \quad A^8 = A^4 \cdot A^4, \quad \ldots.$$

Then compute the desired A^k by using just the necessary powers of 2. For example, if $k = 19$, then $A^{19} = A^{16} \cdot A^2 \cdot A$. This algorithm can be organized so that it uses only a little extra storage and the number of multiplications is $\mathcal{O}(\log k)$.

B. In Grover's algorithm, where we must compute $(W \cdot f)^k \cdot |\phi\rangle$, why not precompute $(W \cdot f)^k$ by repeated squaring?