Bernstein–Vazirani ’93 (p.52), \( f(x) = a \cdot x \equiv \oplus_i a_i x_i \), factor of \( n \) speedup to determine \( a \)

Deutsch ’92 (p.44), factor of 2 speedup to determine whether or not \( 1 \)bit→1bit function \( f(x) \) is constant

Simon ’94 (p.56), \( f(x) = f(x + a) \), measured \( y \) has \( a \cdot y = 0 \) (equivalently \( \sum_i a_i y_i = 0 \) mod2), exponential speedup (\( 2^{n/2} \to O(n) \)) to determine \( a \)

Shor ’94 (p.70), \( f(x) = f(x + r) \), resulting \( y \) is measured with probability \( p(y) = \frac{1}{2^n m} \left| \sum_{k=0}^{m-1} e^{2\pi i k r y/2^n} \right|^2 \), gives \( |y - 2^n/r| < 1/2 \) with \( p > .4 \), sufficient to determine period \( r \) via partial fraction expansion, exponential speedup (\( n2^n, \exp(n^{1/3}) \to O(n^3) \)).

(\( \text{Note: replaces } H^\otimes n |x \rangle = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{i n x \cdot y} |y \rangle \) with \( U_{FT} |x \rangle = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{2\pi i xy/2^n} |y \rangle \).)

Practical application is \( f(x) \equiv b^x \) mod\( N \), where \( b \equiv a^c \) mod\( N \) is an encrypted message, from which \( d' \), satisfying \( cd' \equiv 1 \) mod\( r \), can be calculated, and \( d' \) recovers unencrypted message \( a \equiv b^{d'} \) mod\( N \) (in contrast to using \( d \), with \( cd = 1 \) mod\( (p - 1)(q - 1) \)), where \( N = pq \) and \( r \) divides \( (p - 1)(q - 1) = |G_{pq}| \).

Grover ’96 (p.90), \( f(x) = 1 \) only for \( (m) \) marked value(s) \( x = a \), uses “phase kickback” to express \( U_f \) in terms of \( V = 1 - 2|a\rangle\langle a| \) and \( W = 2|\phi\rangle\langle \phi| - 1 = H^\otimes n (2|0\rangle\langle 0| - 1) H^\otimes n \) is easily constructed. Applying \( \ell \approx \frac{2^{n/2}}{\sqrt{m}} \) times gives probability \( p(a) \approx 1 - O(m/2^n) \), for square-root speedup (\( 2^n/m \to \sqrt{2^n/m} \)).