

Spin effects are used in a number of emerging technologies, of which three deserve a mention: quantum optimal control, quantum information processing, and quantum cryptography. As things stand, only quantum optimal control is used routinely in academic and engineering practice – attempts to implement general-purpose quantum computers and quantum cryptography systems based on spin have failed.

Quantum optimal control

Consider a system with the Hamiltonian partitioned in the following way:

$$\hat{H}(t) = \hat{H}^{(0)} + \sum_n c^{(n)}(t) \hat{H}^{(n)} \quad (1)$$

where $\hat{H}^{(0)}$ is the “drift” that we cannot influence and $c^{(n)}(t)$ are instrumentally controllable coefficients in front of some interaction operators $\hat{H}^{(n)}$ – these are typically electromagnetic fields.

The *optimal control problem* consists in finding such $c^{(n)}(t)$ as would take the system with the best possible accuracy from some initial state $|\psi_0\rangle$ to some destination state $|\sigma\rangle$ with the following constrains:

1. The maximum amplitude of $c^{(n)}(t)$ may be fixed because instruments cannot output arbitrarily strong electromagnetic fields and sample heating must be avoided.
2. The maximum frequency present in $c^{(n)}(t)$ may be fixed because waveform synthesis hardware has a finite switching time and resonators have finite bandwidth.
3. A distribution with respect to $\hat{H}^{(0)}$ may exist in the ensemble because hardware cannot maintain perfect uniformity in the various parameters across the sample.
4. The total time available may be limited or may need to be minimised.

If the control coefficients are discretised on a finite time grid, the Hamiltonian becomes piecewise constant, and the evolution of the system may be calculated by repeatedly applying the exponential solution of Schrödinger’s equation with a constant Hamiltonian:

$$\frac{d}{dt}|\psi\rangle = -i\hat{H}|\psi\rangle \quad \Rightarrow \quad |\psi(t + \Delta t)\rangle = \exp[-i\hat{H}\Delta t]|\psi(t)\rangle \quad (2)$$

The problem may then be cast as maximising the following functional with respect to $c^{(n)}(t)$:

$$J = \text{Re}\langle\sigma|\hat{P}_N \cdots \hat{P}_2 \hat{P}_1|\psi_0\rangle$$

$$\hat{P}_k = \exp\left[-i\left(\hat{H}^{(0)} + \sum_n c^{(n)}(t_k) \hat{H}^{(n)}\right)\Delta t_k\right] \quad (3)$$

If $|\psi_0\rangle$ is transported completely into $|\sigma\rangle$, J would reach the maximum value of 1, otherwise it would return the extent of the wavefunction overlap at the end of the experiment. When the optimisation is accomplished using gradient ascent, the method is called *Gradient Ascent Pulse Engineering* (GRAPE).

In the context of NMR spectroscopy, optimal control pulses are a generalisation of composite pulses. The successes of optimal control theory include ultra-broadband excitation, highly efficient coherence transfer and decoupling, B_0 and B_1 inhomogeneity resilience, and highly selective excitation.

Quantum annealers

At the time of writing, only one type of quantum computing devices is available as finished products on the market – the devices solving a particular type of discrete optimisation problem. Consider a function of multiple discrete variables $f(x_1, x_2, \dots, x_n)$. Because the variables are discrete, the standard gradient descent methods are not available, and it may be demonstrated that no methods exist in classical computing that would be more efficient in general than the very expensive exhaustive search.

Discrete optimisation problems are ubiquitous in physics, mathematics, and computer science: map colouring, semiconductor circuit fault diagnostics, financial portfolio management, drug design, machine learning, *etc.* Many such problems are mathematically equivalent to the problem of finding the lowest energy state of a spin system with the following Hamiltonian:

$$\hat{H} = \sum_k \left(\omega_X^{(k)} S_X^{(k)} + \omega_Y^{(k)} S_Y^{(k)} + \omega_Z^{(k)} S_Z^{(k)} \right) + 2\pi \sum_{k>n} J_{kn} \left(S_X^{(k)} S_X^{(n)} + S_Y^{(k)} S_Y^{(n)} + S_Z^{(k)} S_Z^{(n)} \right) \quad (4)$$

Attempts at hardware implementations based specifically on spin have failed, but systems mathematically identical to spins (arrays of SQUIDs, arrays of optical parametric oscillators) do exist.

In particular, the commercially available *D-Wave* quantum annealer works in the following way:

1. A coupled system of SQUIDs is created with the Zeeman frequencies and the couplings J_{kn} specified by the user. Only a subset of the full Hamiltonian in Equation (4) is available: the couplings are $S_Z^{(k)} S_Z^{(n)}$, and the Zeeman interactions are $S_X^{(k)}$ and $S_Z^{(k)}$.
2. The initial Hamiltonian is set to a simple Zeeman term without couplings, the system is cooled to a temperature that has kT far below the energy gap between the ground state and the first excited state of the Hamiltonian, and allowed to equilibrate.
3. The Hamiltonian is slowly changed: the simple Zeeman term is faded out and the true problem Hamiltonian is faded in. It may be demonstrated that, if the process is sufficiently slow, the system will stay in the instantaneous ground state throughout the process.
4. The final ground state is read out, it corresponds to the minimum energy configuration.

While the academic community (predictably, the spin people) are critical about the claims made by *D-Wave*, it is beyond reasonable doubt that the device works as advertised. An implementation of the same mathematics using optical parametric oscillators is called a *coherent Ising machine*.

Universal quantum computers

While the devices described in the previous section do solve a specific class of problems, they are not programmable in the same sense as classical computers. More precisely, they are not Turing machines. A *universal quantum computer* is a generalisation of a classical Turing machine, where:

1. The set of states is replaced by the Hilbert space (the set of all wavefunctions) of the quantum system, in which superpositions of states are allowed. For example while a “classical” bit only has two states $|0\rangle$ and $|1\rangle$, a “quantum” bit can also be $\alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers; the normalisation condition dictates that $|\alpha|^2 + |\beta|^2 = 1$.
2. The transition between states is accomplished using the quantum equivalent of logic gates – unitary operators of the form $\exp[-i\hat{H}t]$ where \hat{H} is some Hamiltonian.

There are also other, more technical differences and generalisations. Universal quantum computers do not at present exist. An incomplete list of current problems with building them includes:

1. Difficulty creating sufficiently accurate gates. Logical operations in classical computing have thresholds – a charge above a certain level indicates 1, and a charge below that level indicates 0. However, quantum computers must accurately transform the entire Hilbert space each time, resulting in rapid accumulation of errors. One of the most promising ways of generating very accurate gate operations is optimal control theory.
2. Difficulties generating the initial condition, which must be a pure quantum state. This necessitates low temperatures or exotic hardware configurations, for example dynamic nuclear polarisation systems or optical pumps.
3. Difficulties traversing the Hilbert space. Only two-body fundamental interactions exist in nature, meaning that the state space of a quantum system is very sparsely connected. However, the gates required by important quantum algorithms implicitly assume the possibility of arbitrary state space transformations.
4. The inevitable presence of relaxation. The rate of computing is equal to the rate of travel through the state space, which is at best *linear* with each interaction amplitude. However, the rate of relaxation is *quadratic* in the interaction modulation depth by the environmental noise, and often also linear with the number of particles correlated in a particular state.

The task of preventing relaxation amounts to preventing energy dissipation into the environment, which happens to be the definition of the *perpetual motion machine of the third kind* – a delightful irony in light of the history of that particular subject.

5. There are doubts about the very possibility of solving exponentially hard problems with polynomial resources. Solving exponentially hard problems is the *raison d'être* for quantum computers, but thirty years of focused effort would be unlikely to have failed so utterly without a fundamental reason.