4 First steps into quantum computing

In this chapter we discuss two topics: two important early contributions by Feynman and the quantification and creation of entanglement.

4.1 Feynman's point of view

Feynman's two articles from 1982 and 1985 [9, 19] were seminal for the field of quantum computation. Both papers originated from invited talks at conferences. Feynman's interest had been triggered by the notion of reversible computation brought up by Fredkin, Bennett, and Toffoli.
In the first article (which we mentioned already in Chapter 1)Feynman discussed the ways in which physical systems can be simulated by computers. A deterministic simulation of a quantum system on a classical computer runs into problems because the required resources grow exponentially with the system size. Classical (deterministic) dynamics on the other hand is much easier to simulate because it is local, causal, and reversible. Of course such a simulation always involves some kind of discretization for the possible values of time, coordinates, field values, etc.
The deterministic simulation of classical *probabilistic* dynamics suffers from the same problems as quantum dynamics: the necessary resources grow exponentially with system size. This is not completely surprising, since the diffusion equation (a simple example of a probabilistic classical dynamical system)

$$\frac{\partial p}{\partial t} = -\nabla^2 p$$

resembles the free Schrödinger equation, apart from an i. Feynman then discusses the possibility of a *probabilistic simulation* arriving at any possible result with the same probability as the natural process. Of course in that case repeated simulations (plus statistics) would be necessary. It turns out that even a probabilistic simulation of quantum mechanics on a classical computer is impossible. A practical reason is the necessity to keep track of probability densities depending on many variables, but there is also a more important fundamental reason. It is impossible to represent the results of quantum mechanics as results of a classical process containing some "hidden variable", averaged over the possible values of that variable. This can be demonstrated by discussing the EPR (Einstein-Podolsky-Rosen) experiment (polarization measurements on a pair of correlated photons). Quantum mechanics leads to stronger correlations than any classical hidden variable theory. The limits for the correlations in a classical theory are given by Bell's inequality, or the more general CHSH (Clauser, Horne, Shimony, Holt) inequality which has been shown to be violated by many quantum mechanical experiments. We will not discuss these topics here; a nice readable account is found in Chapter 2.6 of Nielsen and Chuang [3].
Feynman's second paper contains quite detailed suggestions for quantum implementations of everyday classical tasks. We will discuss these suggestions up to a "Hamiltonian that adds" before we come to the more fancy quantum applications in the following chapters. The paper also shows that Feynman was well aware of (and interested in) the problems inherent in the high sensitivity of quantum systems to small perturbations; nevertheless, he says: "This study is one of principle; our aim is to exhibit some Hamiltonian for a system which could serve as a computer. We are not concerned with whether we have the most efficient system, nor how we could best implement it."

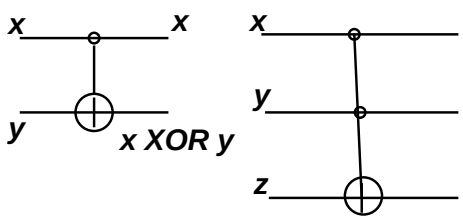

Figure 4.1: Left: Single CNOT gate. Right: CCNOT (Toffoli) gate

From Chapter 2 we know some reversible gates on the 1-, 2-, and 3-bit levels:

$$\text{NOT} \quad \text{maps } x \longrightarrow 1 - x,$$

$$\text{CNOT} \quad \text{maps } (x, y) \longrightarrow (x, x \text{ XOR } y) = \begin{cases} (x, y) \text{ if } x = 0 \\ (x, 1 - y) \text{ if } x = 1 \end{cases},$$

and the Toffoli gate, controlled controlled not or $\theta^{(3)}$ gate:

$$\text{CCNOT maps } (x,y,z) \longrightarrow (x,y,xy \text{ XOR } z) = \begin{cases} (x,y,1-z) \text{ iff } x=y=1 \\ (x,y,z) \text{ otherwise} \end{cases},$$

where "iff" is math lingo for "if and only if", as usual. The two latter gates are shown in figure 4.1.
Note that the symbol $\oplus$ symbolizes XOR or equivalently addition modulo 2. Because for all three gates just one bit is flipped, all three are their own inverses, which will be important in what follows. Viewed as quantum mechanical operators, they are of course also unitary. From these elements we can construct an adder (more precisely, a half adder) which takes two input bits a and b and a carry bit c which is zero initially (Fig. 4.2). The CCNOT changes the carry bit to 1 iff both a and b are 1. The output bit on the middle wire is 1 if $a=1$ and $b=0$ or if $a=0$ and $b=1$ and zero otherwise, and thus yields $a \oplus b$.

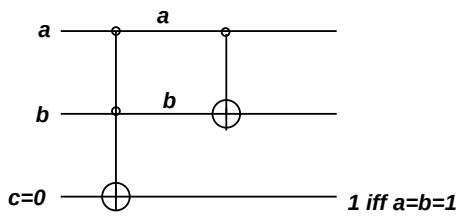

Figure 4.2: An adder (half adder) circuit.

The next circuit (and the one for which we will construct a Hamiltonian) is a full adder (FIG. 4.3). It takes two data bits a and b and a carry bit c from a previous calculation and calculates $a \oplus b \oplus c$, plus a carry bit which is 1 if two or more of a, b, c are 1.

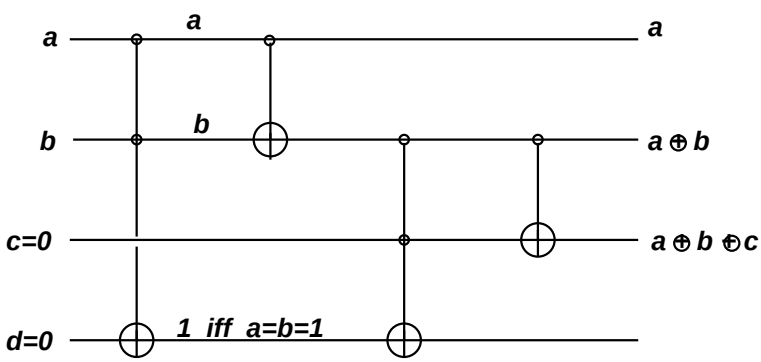

Figure 4.3: A full adder circuit.

What is going on along the three top wires is quite clear, the "tricky bit" is the carry bit d, especially the action of the second CCNOT gate. Note that if $a=b=1$, the control bit $a \oplus b = 0$ so that d is not flipped, even if $c=1$. The only case in which d is flipped (from 0 to 1) is $a \oplus b = 1$ and $c=1$, such that indeed $d=1$ if $a+b+c \geq 2$.
We now map these gates to quantum mechanical operators. To this end we first map the bits to qubits of which we only use the basis states $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\downarrow\rangle$. From Chap. 2 we know how to flip these states by the spin raising and lowering operators:

$$S^+|\downarrow\rangle = |\uparrow\rangle \quad ; \quad S^-|\uparrow\rangle = |\downarrow\rangle.$$

Here it is convenient to use a slightly different language: if we interpret $|0\rangle_a$ and $|1\rangle_a$ as absence and presence of a particle at qubit ("site") a, respectively, and if we use the language of second quantization, that is, creation and annihilation operators:

$$a^\dagger|0\rangle = |1\rangle \quad ; \quad a|1\rangle = |0\rangle,$$

and the number operator

$$a^\dagger a|x\rangle = x|x\rangle \quad (x=0,1).$$

Note that $a^\dagger a + aa^\dagger = 1$, that is, these particles resemble fermions in that no more than one of them can be present. Introducing the same notation for the qubits b and c it is very easy to write down the elementary gates:

$$\text{NOT } (a) = (a + a^\dagger),$$

$$\text{CNOT } (a, b) = (b + b^\dagger)a^\dagger a + 1_b(1_a - a^\dagger a) = (b + b^\dagger)a^\dagger a + 1_b aa^\dagger = (b + b^\dagger - 1_b)a^\dagger a + 1$$

where a is the control bit. In order to avoid sign trouble we assume that operators for different qubits (sites) commute, that is, behave like Bosons in this respect. Together with the Fermi-like on-site commutation relation this shows that these particles are neither Bosons nor Fermions. (Sometimes they are called "hard-core Bosons" or "Paulions".) The mixed commutator structure is cumbersome if standard many-body calculational techniques are to be applied (which we do not intend to). Actually, in some cases of interest these awkward particles can be converted into ordinary Fermions [20]. After the above exercises it is easy to code the Toffoli gate CCNOT as an operator:

$$\theta^{(3)}(a, b, c) = 1 + (c^\dagger + c - 1)a^\dagger a b^\dagger b.$$

The operator for the full adder can be written down reading the diagram in Fig. 4.3 starting from the left and writing down the elementary operators from the right:

$$\text{CNOT } (b, c)\theta^{(3)}(b, c, d) \text{ CNOT } (a, b)\theta^{(3)}(a, b, d)|a, b, c, 0\rangle =: A_4A_3A_2A_1|a, b, c, 0\rangle = \exp\left(-i\frac{\mathbf{H}t}{\hbar}\right)|a, b, c, 0\rangle.$$

Are there a Hamiltonian $\mathbf{H}$ and a time t which satisfy this equation? Obviously this is no easy question, since

$$\exp\left(-i\frac{\mathbf{H}t}{\hbar}\right) = \mathbf{1} + \left(-i\frac{\mathbf{H}t}{\hbar}\right) + \frac{1}{2}\left(-i\frac{\mathbf{H}t}{\hbar}\right)^2 + \frac{1}{6}\left(-i\frac{\mathbf{H}t}{\hbar}\right)^3 + \cdots$$

and thus the right hand side of the above equation for the full adder will be a superposition of states where $\mathbf{H}$ has acted any number of times, from zero to infinity. It turns out that it is possible

- to construct an $\mathbf{H}$ such that the desired final state is present (among others) and
- to separate the desired state from the others.

The trick is to keep a record of which of the A operators have already acted on the input state. This bookkeeping is done by auxiliary (or "slave") particles.
Suppose you want to calculate

$$|\psi_f\rangle = A_k A_{k-1} \cdots A_1|\psi_i\rangle$$

(in our example $k = 4$) for an n-qubit state $|\psi_i\rangle$($n = 4$ in our example). Introduce a "chain" of $k + 1$ new "program counter qubits" named $i = 0 \cdots k$, with corresponding creation and annihilation operators q_i,$q_i^\dagger$. The desired Hamiltonian then reads

$$\mathbf{H} = \sum_{i=0}^{k-1}(q_{i+1}^\dagger q_i A_{i+1} + \text{ h.c.}) = \sum_{i=0}^{k-1}(q_{i+1}^\dagger q_i A_{i+1} + A_{i+1}^\dagger q_i^\dagger q_{i+1}) = \sum_{i=0}^{k-1}(q_{i+1}^\dagger q_i + q_i^\dagger q_{i+1})A_{i+1}.$$

Here, "h.c." denotes the hermitean conjugate (to make $\mathbf{H}$ hermitean). We have used that the A operators are hermitean and that the q operators commute with the A operators. Note that the number of "q particles" $\sum_{i=0}^{k} q_i^\dagger q_i$ is a constant; we will be interested exclusively in the case of a single particle. The action of the Hamiltonian is represented pictorially in Fig. 4.4: Whenever the "program counter particle" moves from site i

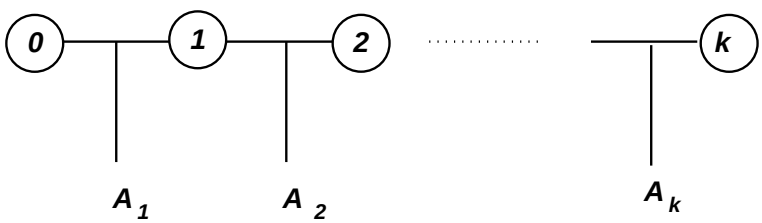

Figure 4.4: A Hamiltonian with register operations A_i.

to $i + 1$ or vice versa the operator A_{i+1} acts on the "register qubits" where the calculation is performed. The

calculation starts with the register qubits in the input state $|\psi_i\rangle$ and the program counter particle at site 0. The action of $\mathbf{H}^\nu$ then yields

$$\mathbf{H}^\nu|1000\cdots0\rangle|\psi_i\rangle = \mathbf{H}^{\nu-1}|0100\cdots0\rangle A_1|\psi_i\rangle = \mathbf{H}^{\nu-2}\left(|0010\cdots0\rangle A_2A_1|\psi_i\rangle + |1000\cdots0\rangle \underbrace{A_1A_1}_{\mathbf{1}}|\psi_i\rangle\right) = \cdots$$

We see that if the program counter particle is at site l, the last operator which has been active is A_l:

$$|0\cdots\underbrace{1}_{l}\cdots0\rangle A_l\cdots|\psi_i\rangle.$$

The next application of $\mathbf{H}$ then leads to two possibilities:

- $l \to l-1; A_l$ is squared (=erased)
- $l \to l-1; A_{l+1}$ is prepended to the string of A operators.

(This argument can of course be transformed into a rigorous proof by induction.) We conclude that if our final state contains a component with the counter particle at site k, we are finished. We only have to project out the desired component:

$$\alpha|00\cdots01\rangle|\psi_f\rangle = q_k^\dagger q_k \exp\left(-i\frac{\mathbf{H}t}{\hbar}\right)|100\cdots0\rangle|\psi_i\rangle,$$

where α is a normalization factor whose size may be important in practice.
Exercise: Construct the Hamiltonian for the full adder. Calculate (for example numerically, with your good old classical PC) the amplitude of the desired output state as a function of time. Does this amplitude depend on the contents of the register qubits? Can you see how it will depend on the number of program steps k for more general programs? Warning: I haven't done this exercise myself, but I am confident that it is feasible and that it will basically reduce to finding the eigenvalues and eigenstates of a single particle on an open-ended 5-site tight-binding chain, which is a typical (and solvable) exercise in many courses on condensed matter theory.
After showing how to construct the Hamiltonian, Feynman in his paper then goes on to discuss the influence of imperfections (for example not perfectly equal bond strengths in the program counter chain), simplifications of the implementation and more complicated tasks like implementing loops which perform a piece of code a given number of times. We will do something different.

4.2 Entanglement: generation and quantification

In Chapter 1 we had examples of entangled states, but no general definition of entanglement. We roughly equated entanglement with correlation, but we shall see soon that that is not quite correct. For a bipartite system we said that an entangled state is not a product state. The question is how to recognize a product state if you see one. Is

$$|\psi\rangle = \frac{1}{2}(|\uparrow\uparrow\rangle - |\downarrow\downarrow\rangle - |\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$$

a product state? (It is.)
Consider, as in Chapter 1, a system with subsystems A and B, and an arbitrary pure state

$$|\psi\rangle_{AB} = \sum_{i,\mu} a_{i,\mu}|i\rangle_A|\mu\rangle_B = \sum_i |i\rangle_A|\tilde{i}\rangle_B \quad (|\tilde{i}\rangle_B := \sum_\mu a_{i\mu}|\mu\rangle_B),$$

where $\{|i\rangle_A\}$ and $\{|\mu\rangle_B\}$ are bases (that is, orthonormal) for the Hilbert spaces of A and B, respectively. The $|\tilde{i}\rangle_B$ are *not* necessarily orthogonal or normalized. Let $\{|i\rangle_A\}$ be the basis in which the reduced density matrix of subsystem A is diagonal:

$$\rho_A = \sum_i p_i|i\rangle_{AA}\langle i|.$$

Compare this with the expression obtained from ρ_A as computed by the partial trace over B:

$$\rho_A = \mathrm{Tr}_B(|\psi\rangle_{ABAB}\langle\psi|) = \mathrm{Tr}_B\left(\sum_{ij}|i\rangle_{AA}\langle j|\otimes|\tilde{i}\rangle_{BB}\langle\tilde{j}|\right) = \sum_{ij} {}_B\langle\tilde{j}|\tilde{i}\rangle_B(|i\rangle_{AA}\langle j|).$$

(Note that $\mathrm{Tr}\,|\phi\rangle_{BB}\langle\psi| = \sum_\mu {}_B\langle\mu|\phi\rangle_{BB}\langle\psi|\mu\rangle = {}_B\langle\psi|\phi\rangle_B$ by exchanging factors and using the completeness of $\{|\mu\rangle_B\}$.) A comparison of the two forms of ρ_A shows

$${}_B\langle\tilde{j}|\tilde{i}\rangle_B = p_i\delta_{ij}$$

Thus the $|\tilde{i}\rangle_B$ *are* in fact orthogonal; we normalize them by rescaling

$$|i'\rangle_B = p_i^{-1/2}|\tilde{i}\rangle_B.$$

In terms of this particular orthonormal basis (for A and B) we have

$$|\psi\rangle_{AB} = \sum_i \sqrt{p_i}|i\rangle_A|i'\rangle_B$$

the **Schmidt decomposition** of the bipartite pure state $|\psi\rangle_{AB}$. Note that the basis in which a $|\psi\rangle$ has this form depends on $|\psi\rangle$.
From the partial trace over the Hilbert space of A we get

$$\rho_B = \mathrm{Tr}_A(|\psi\rangle_{ABAB}\langle\psi|) = \sum_i p_i|i'\rangle_{BB}\langle i'|$$

and thus ρ_A and ρ_B have the same number of nonzero eigenvalues. The number of zero eigenvalues (and thus the dimensions of the A and B subspaces) may differ. If the nonzero eigenvalues of ρ_A (and ρ_B) are all nondegenerate, the Schmidt decomposition can be determined uniquely (by diagonalizing ρ_A and ρ_B). If not, there is some ambiguity (as usual in the case of degeneracy), see [7], Sec. 2.4.
The number of nonzero eigenvalues of ρ_A (or ρ_B) is called the *Schmidt number*. If the Schmidt number is greater than 1, the state is *entangled*, otherwise it is separable.
The reduced density matrices of an entangled state are mixed:

$$\mathrm{Tr}(\rho_A)^2 = \mathrm{Tr}(\rho_B)^2 = \sum_i p_i^2 < \sum_i p_i = 1$$

because $x^2 < x$ for $0 < x < 1$. The reduced density matrices of a separable state are pure.
Entanglement is not equal to correlation: $|\uparrow\rangle_A|\uparrow\rangle_B$ is certainly correlated, but not entangled. This state can be created by two subsystem owners Alice and Bob even if they are far apart. To turn this state into an entangled one like $\frac{1}{\sqrt{2}}(|\uparrow\rangle|\uparrow\rangle + |\downarrow\rangle|\downarrow\rangle)$ requires a *global* unitary transformation, that is, one that cannot be written as $U_A \otimes U_B$; such a local transformation obviously cannot change the Schmidt number of a state. Note that the notions of separability and entanglement may be generalized from pure to mixed states; we shall discuss that later if necessary.

4.2.1 Creation of entanglement: Computer scientist style

Just use some suitable gates, for example the CNOT gate and the Hadamard gate

$$\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

to create the famous *Bell states*

$$|\beta_{ab}\rangle = \text{ CNOT } (a,b)\mathbf{H}(a)|a,b\rangle$$

An example:

$$\mathbf{H}(a)|0,0\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,0\rangle) \Rightarrow |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle).$$

The other members of the *Bell basis*:

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle - |1,1\rangle)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|0,1\rangle - |1,0\rangle)$$

4.2.2 Creation of entanglement: Physicist style

Of course physicists use not gates but *interactions*. To understand what is going on we need a little refresher on the fundamentals of exchange interaction, singlet and triplet states.
Consider two spins $\frac{1}{2}$, (a,b) and calculate the square of the total spin:

$$\vec{S}_T^2 = (\vec{S}_a + \vec{S}_b)^2 = \frac{1}{2}(\frac{1}{2}+1)\hbar^2 + \frac{1}{2}(\frac{1}{2}+1)\hbar^2 + 2\vec{S}_a \cdot \vec{S}_b = \frac{3}{2}\hbar^2 + 2\vec{S}_a \cdot \vec{S}_b$$

Now S_T can be 0 or 1; for $S_T = 1, S_T^z$ can be $\pm 1, 0$ (triplet), and for $S_T = 0, S_T^z = 0$ (singlet). The singlet state is

$$|S\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle).$$

(Note that both the total spin raising operator $S_a^+ + S_b^+$ and the total spin lowering operator $S_a^- + S_b^-$ annihilate this state; so it must be the $S_T = 0$ state.)
The triplet states are $|\uparrow\uparrow\rangle$, $|\downarrow\downarrow\rangle$ (obvious) and $|T\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$ (orthogonal to $|S\rangle$). We write the *exchange interaction* (Heisenberg)

$$\vec{S}_a \cdot \vec{S}_b = \frac{\hbar^2}{2} S_T(S_T+1) - \frac{3}{4}\hbar^2 = \begin{cases} +\frac{1}{4}\hbar^2 & (S_T = 1, \text{ triplet }) \\ -\frac{3}{4}\hbar^2 & (S_T = 0, \text{ singlet }) \end{cases}.$$

The singlet and triplet states are thus eigenstates of the exchange interaction, with different energies. That is all we need from magnetism. We take an initial state $|\uparrow\downarrow\rangle$ (which is certainly not entangled) and let it evolve under the action of an antiferromagnetic exchange coupling between the two spins:

$$\mathbf{H} = \frac{\omega}{\hbar}\vec{S}_a \cdot \vec{S}_b$$

$$|\psi(t)\rangle = \exp\left(-i\frac{\mathbf{H}t}{\hbar}\right)|\uparrow\downarrow\rangle = \frac{1}{\sqrt{2}}\exp\left(-i\frac{\mathbf{H}t}{\hbar}\right)(|T\rangle + |S\rangle) = \frac{1}{\sqrt{2}}\left(\exp(-i\frac{\omega}{4}t)|T\rangle + \exp(+i\frac{3}{4}\omega t)|S\rangle\right) =$$

$$\frac{\exp(-i\frac{\omega}{4}t)}{\sqrt{2}}(|T\rangle + \exp(i\omega t)|S\rangle) = \frac{\exp(-i\frac{\omega}{4}t)}{2}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle + \exp(i\omega t)|\uparrow\downarrow\rangle - \exp(i\omega t)|\downarrow\uparrow\rangle) =$$

$$\frac{\exp(-i\frac{\omega}{4}t)}{2}\left((1+\exp(i\omega t)|\uparrow\downarrow\rangle + (1-\exp(i\omega t)|\downarrow\uparrow\rangle\right).$$

This is a bipartite pure state. Let us calculate its Schmidt number.

$$|\psi(t)\rangle\langle\psi(t)| = \frac{1}{4}\left(|\uparrow\downarrow\rangle\langle\uparrow\downarrow| \, |1+\exp(i\omega t)|^2 + |\downarrow\uparrow\rangle\langle\downarrow\uparrow| \, |1-\exp(i\omega t)|^2 + \right.$$

$$\left. |\uparrow\downarrow\rangle\langle\downarrow\uparrow| (1+\exp(i\omega t))(1-\exp(-i\omega t)) + |\downarrow\uparrow\rangle\langle\uparrow\downarrow| (1-\exp(i\omega t))(1+\exp(-i\omega t))\right)$$

and thus

$$\rho_a = \mathrm{Tr}_b\,|\psi(t)\rangle\langle\psi(t)| = \frac{1}{4}(|\uparrow\rangle\langle\uparrow| \, |1+\exp(i\omega t)|^2 + |\downarrow\rangle\langle\downarrow| \, |1-\exp(i\omega t)|^2) = \frac{1}{4}\begin{pmatrix} |1+\exp(i\omega t)|^2 & 0 \\ 0 & |1-\exp(i\omega t)|^2 \end{pmatrix}$$

For $\exp(i\omega t) = \pm 1$ the Schmidt number is 1, otherwise it is 2: "entanglement oscillations". As predicted in Chapter 1, *interaction creates entanglement.*
Of course, the computer scientist's way to create entanglement can also be rephrased in terms of interactions, but these do not look very physical. We know that the Hadamard gate is the sum of X and Z, and from the Feynman discussion we can easily see that

$$\text{CNOT } (a,b) = (X - \mathbf{1})_b \frac{1}{2}(Z + \mathbf{1})_a + \mathbf{1}_{ab}.$$

Entanglement is an important ingredient in many quantum communication, state teleportation etc. schemes which we will discuss later. Here we have only treated two-particle entanglement. Three-particle entanglement has been known for some time as "Greenberger-Horne-Zeilinger" (GHZ) correlation and was observed[21] in 2000. Entanglement of four particles was achieved in an ion trap using laser pulse techniques[22, 23]. The method (according to the authors) is scalable to larger numbers of particles and can produce entanglement "on demand". The state created is $|\uparrow\uparrow\uparrow\uparrow\rangle + |\downarrow\downarrow\downarrow\downarrow\rangle$. Even more recently[24, 25], a single light pulse interacting with two clouds of about 10^{12} Cs atoms each was used to entangle the two clouds for half a millisecond. From my (JS) very superficial look at the paper I am not sure what the exact nature of the entangled state was.
The only *measure* of entanglement we have discussed up to now is the Schmidt number which is defined only for bipartite systems and provides only a yes/no information about entanglement. More quantitative measures of entanglement and generalizations to larger systems are being widely discussed in the reseearch literature.