Innovation Kick – Quantum Computing:

Gate-based Quantum Computing und Quantum Annealing – zwei Wege zu Quantenanwendungen

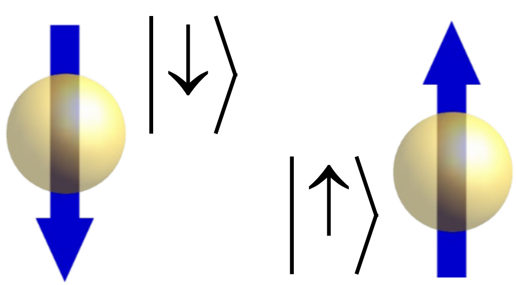
R. M. Füchslin

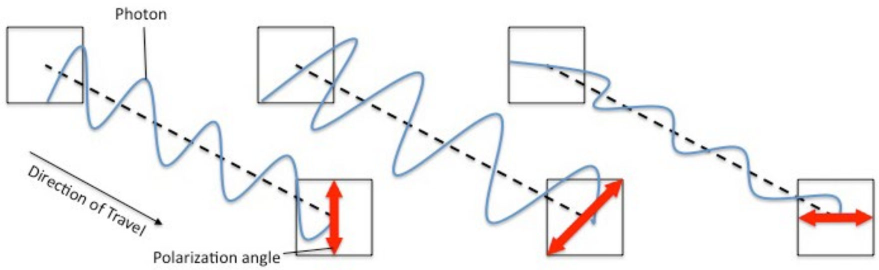
April 4, Technopark Winterthur

Qubit

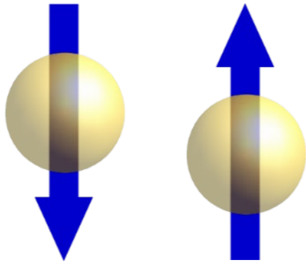
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Rightarrow |\psi\rangle = c_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = c_0|0\rangle + c_1|1\rangle \qquad |c_0|^2 + |c_1|^2 = 1$$

- **Qubit:** abstrakte Datenstruktur in einem zweidimensionalen komplexen Vektorraum.
- Koeffizienten c_k sind komplexe Zahlen: $c_k = a_k + ib_k$
- Physikalische Realisierung: Zwei-Zustands-System wie polarisierte Photonen oder Elektronen.





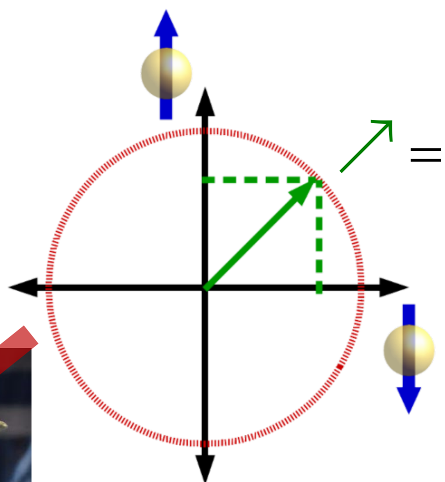
Qubits = “Gemischte” Bits?



$|\downarrow\rangle \qquad |\uparrow\rangle$

“Rein”

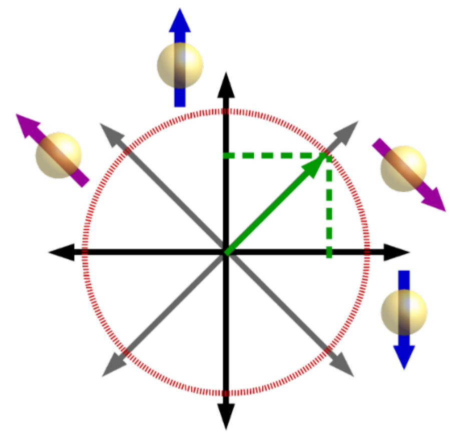
- Spins können irgendeine Richtung haben.
- **Darstellung des Vektors** hängt von der Wahl des Koordinatensystems ab.
- «Gemischt» zu sein ist keine Eigenschaft des Teilchens, sondern des Koordinatensystems.
- ➔ «Gemischt» zu sein, ist gar nichts spezielles!



$$\nearrow = \frac{1}{\sqrt{2}}\left(|\downarrow\rangle + |\uparrow\rangle\right)$$

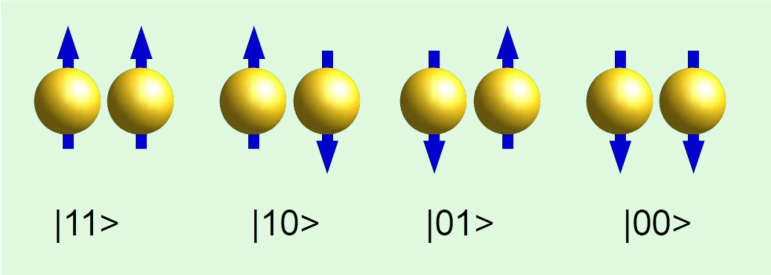
“Gemischt”

$$\nearrow = |\downarrow\rangle$$



“Rein” (dem Elektron ist unsere Wahl der Koordinaten völlig egal).

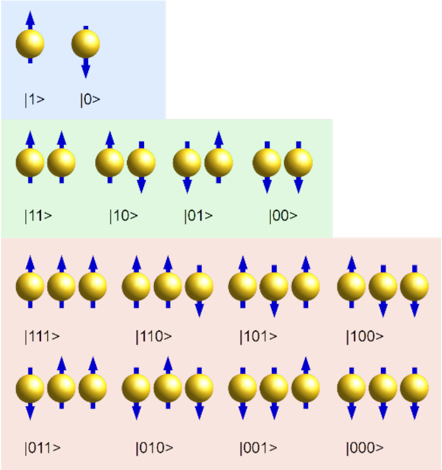
Gekoppelte Qubits



$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$
$$|c_{00}|^2 + |c_{01}|^2 + |c_{10}|^2 + |c_{11}|^2 = 1$$

- Ein System aus zwei gekoppelten Qubits wird dargestellt durch einen Vektor in einem Zustandsraum mit vier (komplexen) Dimensionen

Quantenregister



- **Gekoppelte Qubits den Inhalt eines Quantenregister.**
- **Ein klassisches Register befindet sich immer in einem Basiszustand.**
- **Ein Quantenregister kann eine Mischung von Basiszuständen darstellen!**
- **Ein Basiszustand steht für eine Bitsequenz.**

$$|\psi\rangle = c_{000}|000\rangle + c_{001}|001\rangle + c_{010}|010\rangle + c_{011}|011\rangle$$
$$+ c_{100}|100\rangle + c_{101}|101\rangle + c_{110}|110\rangle + c_{111}|111\rangle$$
$$|c_{000}|^2 + |c_{001}|^2 + |c_{010}|^2 + |c_{011}|^2 + |c_{100}|^2 + |c_{101}|^2 + |c_{110}|^2 + |c_{111}|^2 = 1$$

n Spins bilden einen 2^n - dimensionalen Zustandsraum.

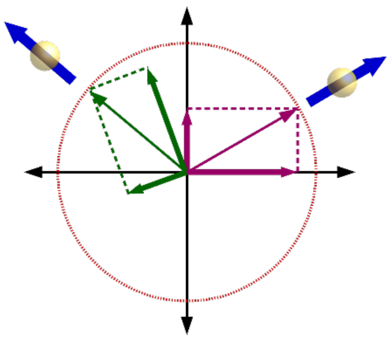
Operationen auf Quantenregistern

- **Messung $\boldsymbol{M}$** in einer Basis $|b_0>, \dots, |b_m>$

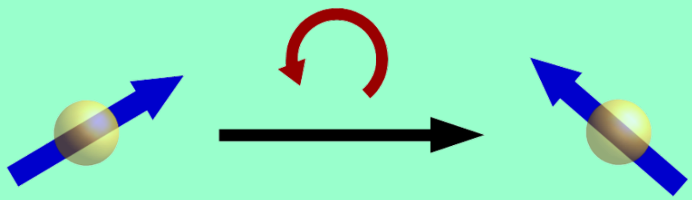
$$|\psi\rangle = \sum_{k=0}^{2^n-1} c_k |b_k\rangle \quad \Rightarrow \quad M|\psi\rangle = |b_x\rangle \text{ with probability } |c_x|^2$$

- Deswegen gilt $\sum_{k=0}^{2^n-1} |c_k|^2 = 1$
- ➔ Länge eines Quantenregisters ist immer gleich (gleich 1)
- Weniger langweilig als es scheint: **Unitäre Transformationen** sind einfach **Rotationen von $|\psi>$.**
- Bemerkung: Rotationen können rückgängig gemacht warden, Messung ist irreversibel.

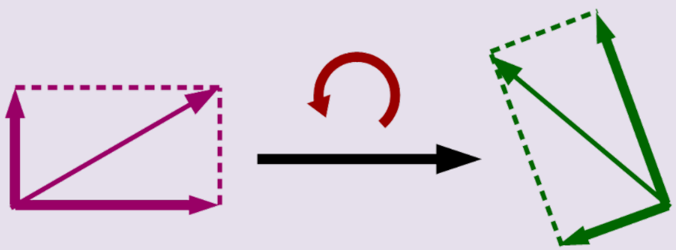
Quantenparallelismus



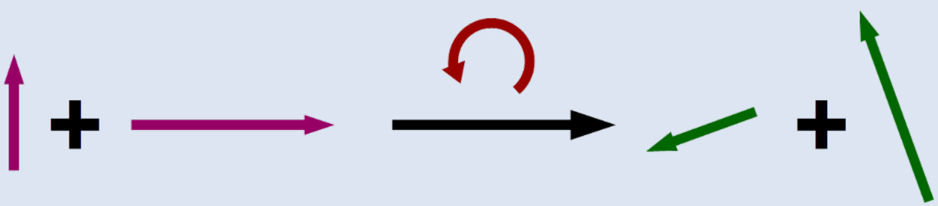
Operation auf einem Qubit



Die Operation ist ein physikalischer Prozess. Das Elektron weiss nichts von Koordinaten



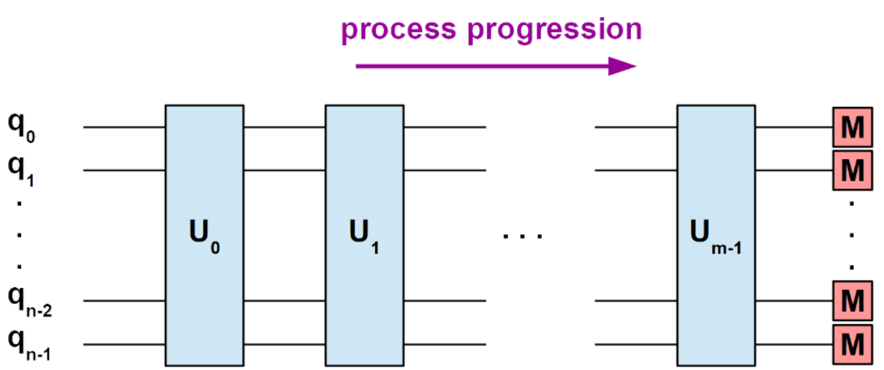
Als Datenstruktur wird ein Vektor bestehend aus zwei Koordinatenvektoren rotiert.



Für uns, wenn wir in einer Basis messen, sieht es aus, als ob die Basisvektoren alle zusammen rotiert warden.

Ein Quantenschaltkreis

- Ein Quantenschaltkreis:



- Wir präparieren am Anfang ein paar Qubits.
- Wir führen eine Reihe von unitären Transformationen U_i auf dem Quantenregister durch.

$$M(U_{m-1}U_{m-2}\ldots U_1U_0|\Psi_{in}\rangle)$$

- Die Berechnung endet mit einer Messung M.
- **Die Drähte darf man nicht wörtlich nehmen!** Wir verschieben das Quantenregister nicht von links nach rechts. Wir wenden eine Reihe von Transformationen auf den Eingabezustand an.

Wozu das Ganze?

- Grundsätzlich: Quantenalgorithmen sind in der Regel sog. **stochastische Algorithmen**. ➔ Man lässt den Algorithmus mehrfach laufen, und macht ein majority voting.
- Das liegt nicht nur an der hohen Fehleranfälligkeit, sondern auch an der grundsätzlich stochastischen Natur des Messprozesses.
- **Wichtig: Quantencomputer können nicht mehr als klassische Computer, aber sie können es schneller.**
- Berühmte, konzeptuell wichtige aber praktisch nutzlose Beispiele:
  - Grover - Algorithmus
  - Deutsch - Algorithmus
  - Bernstein – Vazirani Algorithmus
  - **Shor – Algorithmus**

A. Capone

Verschränkung

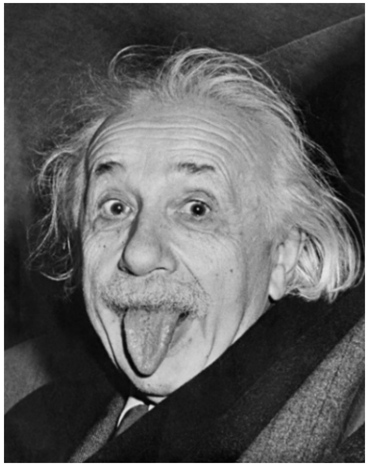
- **Verschränkte Zustände** eines Zwei-Qubit-Registers sind Zustände, die NICHT als Produkt zweier einzelner Qubits verstanden werden können

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \neq \left(\alpha|0\rangle + \beta|1\rangle\right) \otimes \left(\gamma|0\rangle + \delta|1\rangle\right)$$

$$\begin{aligned}&\left(\alpha|0\rangle + \beta|1\rangle\right) \otimes \left(\gamma|0\rangle + \delta|1\rangle\right)\\ &\qquad = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle\end{aligned}$$

Es gibt keine Zahlen $\alpha, \beta, \gamma, \delta$ so, dass

$$\alpha\gamma = 1, \quad \alpha\delta = 0, \quad \beta\gamma = 0, \quad \beta\delta = 1$$



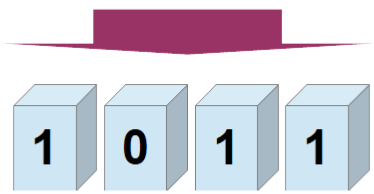
A. Einstein
Lehrbeauftragter a.D. am Technikum Winterthur.

Bits vs. Qubits

Zurich University of Applied Sciences
zh aw School of Engineering

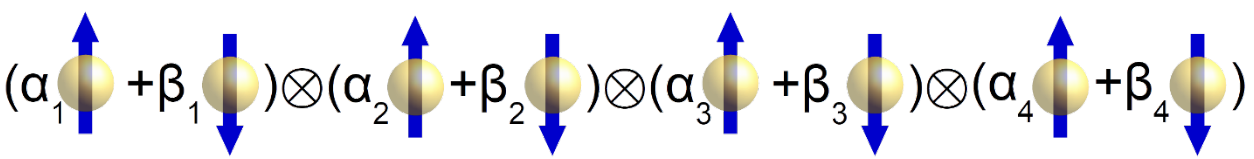
1011

Klassischer Computer: Register = Sequenz von Bits.



Quantenregister: i.A. keine Sequenz von Qubits!

$$|\psi\rangle = c_{0000}|0000\rangle + c_{0001}|0001\rangle + \ldots + c_{1111}|1111\rangle$$



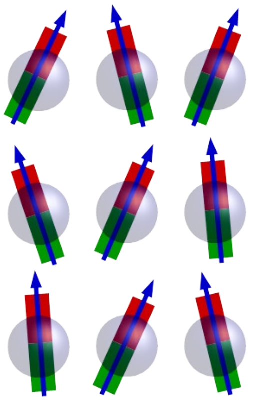
Quantencomputing =
Parallelismus PLUS Verschränkung!

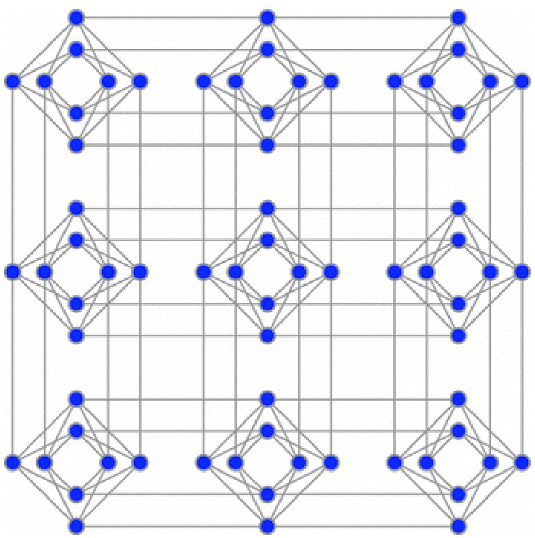
Mehr Physik wagen!

Zurich University of Applied Sciences
School of Engineering

- Fakt 1: Physikalische Systeme beinhalten Energie E.
- Fakt 2: Jedes System hat einen Zustand mit minimaler Energie.
- Fakt 3: Wir können Spins / Qubits koppeln. Die Energie E ist gleich:

$$E = \sum_i h_i q_i + \sum_{i,j} K_{ij} q_i q_j$$





Mehr Physik wagen!

Grundidee: In einem Quantum annealer wählen wir h_i und K_{ij} so, dass das Energieminimum des Spinsystems, also irgendeine Qubit - Konfiguration, z.B.

$$q_1 = 0, q_1 = 1, q_2 = 1, \ldots, q_n = 1$$

$$E = \sum_i h_i q_i + \sum_{i,j} K_{ij} q_i q_j$$

der Lösung eines Optimierungsproblems entspricht.

Ising formulations of many NP problems

Andrew Lucas
Department of Physics, Harvard University, Cambridge, MA, USA 02138

We provide Ising formulations for many NP-complete and NP-hard problems, including all of Karp's 21 NP-complete problems. This collects and extends mappings to the Ising model from partitioning, covering and satisfiability. In each case, the required number of spins is at most cubic in the size of the problem. This work may be useful in designing adiabatic quantum optimization algorithms.

lucas@fas.harvard.edu

January 27, 2014

Vertex cover

Traveling sales man

Subset sum

Graph coloring

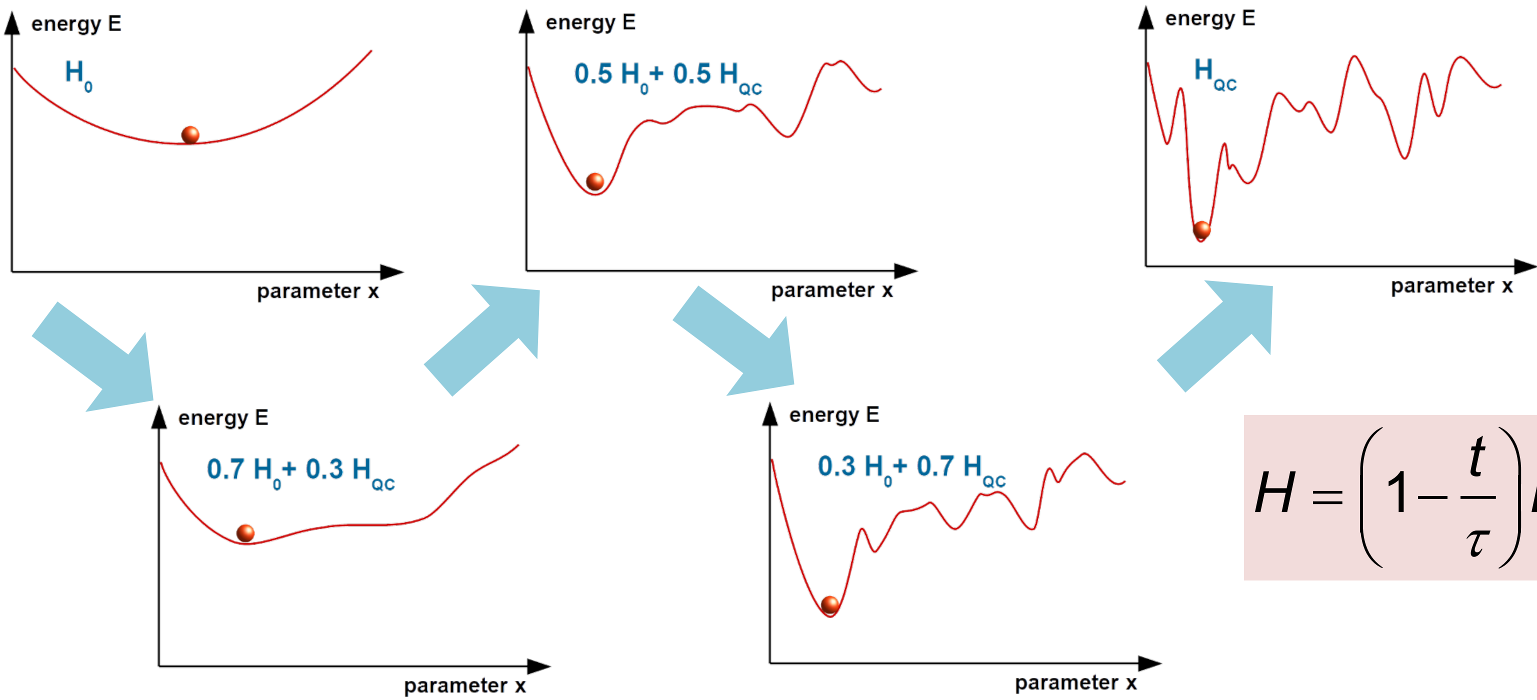
Number partitioning

Knapsack packing

Satisfiability

Quantum Annealing:

Befindet sich ein System im Zustand mit tiefster Energie und wird das System genügend langsam verändert (damit auch die Lage des tiefsten Energiezustands), bleibt das System im energetisch tiefsten Zustand.



$$H = \left(1 - \frac{t}{\tau}\right) H_0 + \frac{t}{\tau} H_{QC}$$

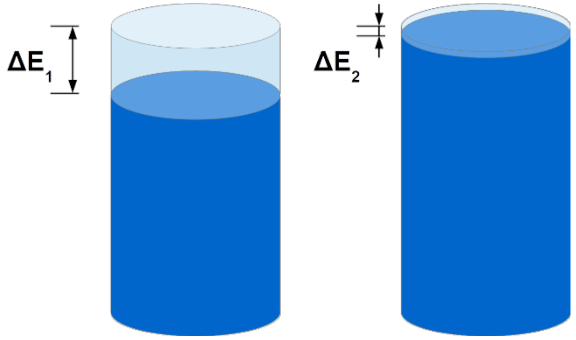
“Genügend langsam” ???

- Einige sehr grundlegende Überlegungen führen zu der Schlussfolgerung, daß für ein Problem der Größe N für die Übergangszeit T gilt:

$$\tau = O\left(\exp\left(\alpha N^{\beta}\right)\right)$$

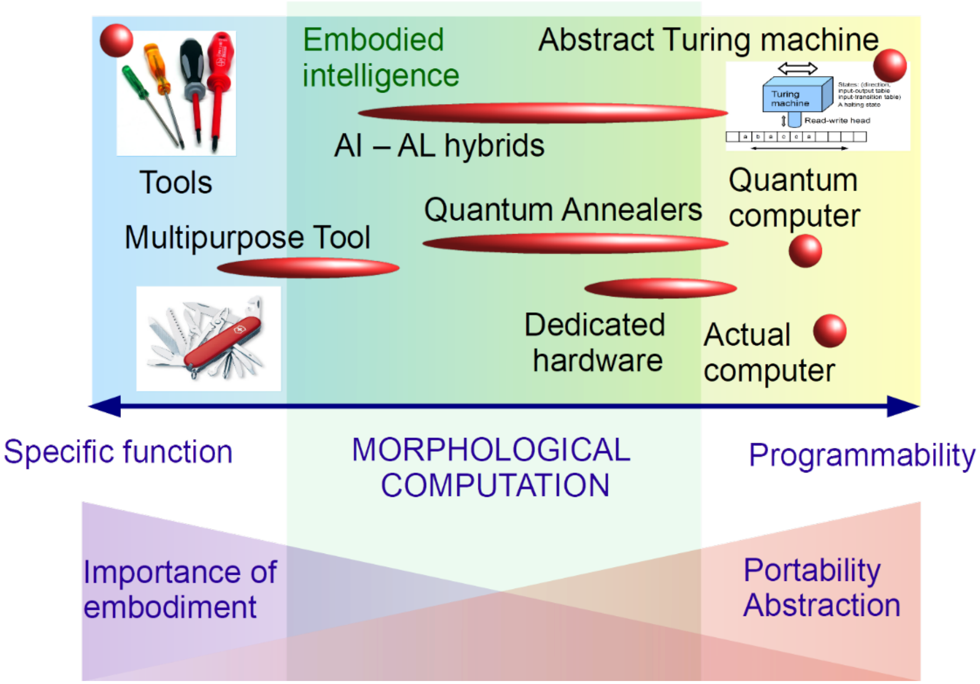
$$H = \left(1 - \frac{t}{\tau}\right) H_0 + \frac{t}{\tau} H_{QC}$$

- Das heisst: Die «Rechendauer» steigt immer noch exponentiell
- Hoffnung und Ziel: α oder β kann man klein halten.
- Konkret geht es um die energetische Differenz zwischen dem tiefsten und dem zweittiefsten Energiezustand: **Je grösser die «Energielücke» desto schneller kann der Quantum Annealer gefahren werden.**



Summary

- Verschiedene Wege führen zum Quantencomputing!
- Gate-based Quantencomputing:
  - Kann theoretisch sehr viel!
  - **Error – correction nötig**
  - Programmierung erfordert wenig Hardwarekenntnisse
- Quantenannealer:
  - Kann nicht alles, aber viel!
  - Physik spielt eine Rolle: Programmierung kann nicht von Hardware getrennt warden.
  - **Die Physik ist schon drin!**



Kontakt

Prof. Dr. Rudolf M. Füchslin
Institute for Applied Mathematics and Physics
Head of Group for Applied Complex Systems Sciences
Zurich University of Applied Sciences
TP 216 - Technikumstr. 9
CH-8401 Winterthur, Switzerland
www.zhaw.ch/iamp

European Centre for Living Technology
Co - director
Ca' Bottacin
Dorsoduro 3911,
30123 Venice Italy
http://www.ecltech.org/

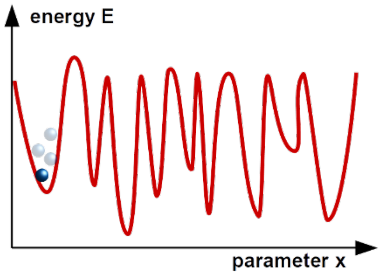
Office: +41(0)58 934 75 92
+39 0 41 234 75 94
Mobile: +41(0)79 232 74 36

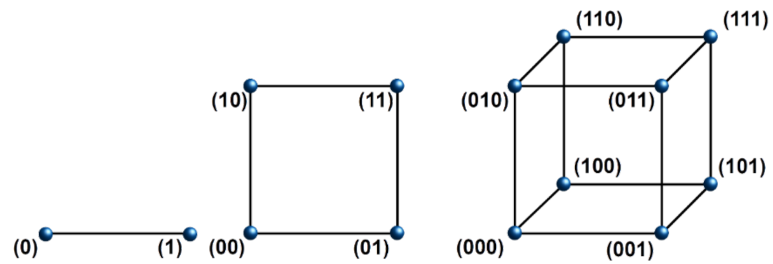
Skype : rudolf.marcel.fuechslin

rudolf.fuechslin@zhaw.ch

We ♥ hochdimensionale Räume!

- Man kann sich fragen, was passiert, wenn das Minimum "weit entfernt" vom ursprünglichen Grundzustand ist.





- 2D - Plots führen in die Irre. Die wahre Fitnesslandschaft existiert auf einem n-dimensionalen Würfels. ➔ Jeder ist nah an allem anderen.
- Und falls es doch mal Probleme geht: Dann wird getunnelt!