Quantum Information Theory: MAT 4953 XLS 5983. Lesson 09 (Nov 15-17), Fall 2022.

José A. Morales E., UTSA Math and Physics & A. Depts.

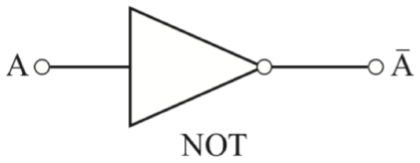
Abstract

Quantum gates & circuits

1. Quantum gates & circuits

1.1. Classical Digital Electronics

In "classical" digital electronics (the standard one) the logical bits 0,1 are encoded as voltages. A zero (ground) voltage for 0, and a high voltage for 1. The bits are manipulated by devices (based on transistors) which are called gates. There are single-bit and two-bit gates. There exists only a single-bit gate, which is called the NOT gate (it flips the given logical bit into the other one, so in Boolean logic is like a negation). It's represented by the following diagram:



A	Ā
0	1
1	0

Figure: From "Quantum gates & circuits", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

Regarding the two-bit gates, the simplest ones are the AND and OR gates. They are represented in the following diagram:

Email address: jose.morales4@utsa.edu (José A. Morales E., UTSA Math and Physics & A. Depts.)

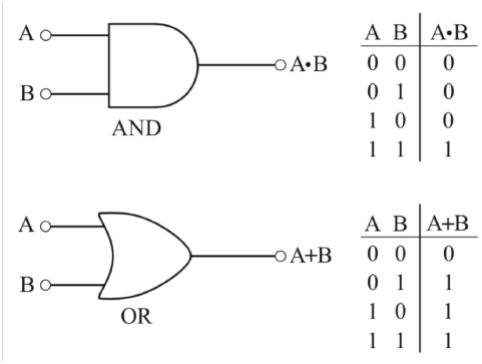


Figure: From "Quantum gates & circuits", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

If one combines the AND, OR with a NOT gate, that would give the NAND, NOR gates (negative-and, negative or).

Remark 1. The two-bit gates abovementioned (AND, OR) together with the single-bit NOT gate allow us to perform ANY LOGICAL operation on a string of bits in classical digital electronics. This is what we mean by a computation: a logical operation.

1.2. Single-qubit quantum gates: Examples

Now we consider single-QUBIT gates appearing in quantum computations. There are more than one (as opposed to classical computing), because a qubit is generally a superposition of the two basis states $|0\rangle, |1\rangle$. We have seen some examples before actually: for example, the Hadamard gate, the Pauli-X, Pauli-Y, Pauli-Z operators, etc. Some other examples are the Phase gate and the $\pi/8$ one. We present all these examples in the following diagram:

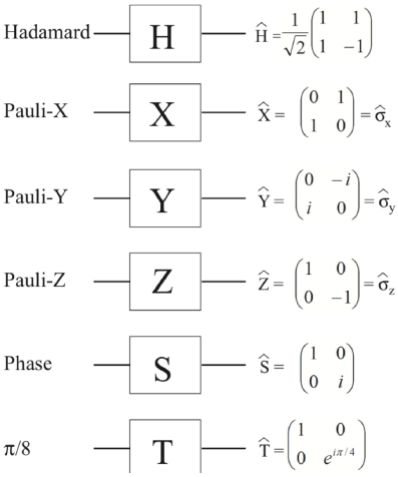


Fig. From "Quantum gates & circuits", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

A single qubit gate may perform any single-qubit unitary transformation: that is, any rotation on the Bloch sphere.

Remark 2. A fundamental difference between classical and quantum gates is that quantum ones can only perform UNITARY operations, whereas classical gates don't need to do so.

1.3. Two-qubit quantum gates

These types of gates need to have two output qubits (as opposed to their classical counterparts) given the two input qubits so that they represent unitary operations. Though there are many of these type, one of the most important is the CNOT (controlled NOT) gate, which is represented in the diagram below:

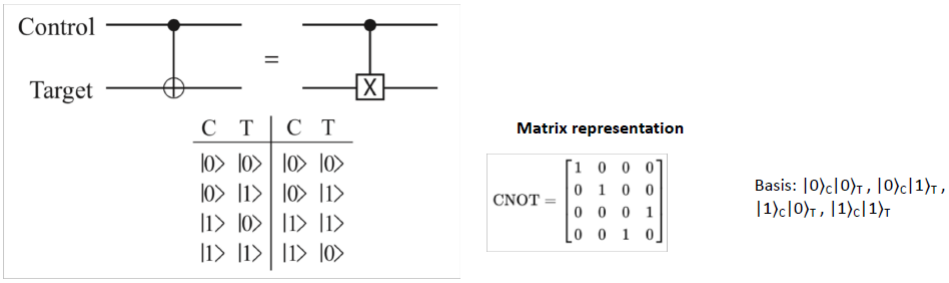


Figure: From "Quantum gates & circuits", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

The main idea behind this gate is that the first qubit acts as a "control qubit", whose state determines if there's a flip (sending $|0\rangle$ to $|1\rangle$ and viceversa, as in a NOT) to the second qubit (if qubit 1 is in state $|1\rangle$) or if the system is unchanged (if the control qubit is in state $|0\rangle$). This can be schematically summarized by the following mapping,

$$|A\rangle \otimes |B\rangle \rightarrow |A\rangle \otimes |B \oplus A\rangle \,,$$

where $\oplus$ represents the "Addition modulo 2". The CNOT gate is induced by the following unitary operator (by linearity):

$$\widehat{U}_{CNOT} = |0\rangle \langle 0| \otimes \widehat{I} + |1\rangle \langle 1| \otimes \widehat{\sigma}_x$$

In fact, the CNOT gate can generate entanglement. If the control qubit is in a superposition, then it implements the following transformation:

$$\frac{|0\rangle_C + |1\rangle_C}{\sqrt{2}} \otimes |0\rangle_T = \frac{|0\rangle_C \otimes |0\rangle_T + |1\rangle_C \otimes |0\rangle_T}{\sqrt{2}} \rightarrow \frac{|0\rangle_C \otimes |0\rangle_T + |1\rangle_C \otimes |1\rangle_T}{\sqrt{2}}$$

noticing that in the left we have an unentangled (product) state, and on the right we have the Bell state $|\Phi^+\rangle$.

Remark 3. In both classical digital and quantum computation a small number of gates can be used to perform any operation. In the Quantum case, we only need the one-qubit gates plus a single two-qubit gate (such as CNOT).

Proof. The proof of the remark above can be found in the course textbook. □

The CNOT gate is an example of a universal two-qubit gate.

Example 4. Controlled unitary gates:

Any CONTROLLED-UNITARY gate (TBD) can be realized using at most 2 CNOT gates and 4 single-qubit gates. To prove it, remember that the most general single-qubit unitary operator is

$$\widehat{U} = e^{i\alpha}(\cos(\beta)\widehat{I} + i\sin(\beta)\vec{n}\cdot\vec{\widehat{\sigma}}),$$

where α and β are real, and $\vec{n}$ is a unit vector. A controlled unitary gate can be assembled in the following way, noticing that the highlighted operator multiplies the upper qubit (so the entire state vector) by $\exp(i\alpha)$ if the control qubit is in the state $|1\rangle$ and does nothing if the control qubit is in the state $|0\rangle$:

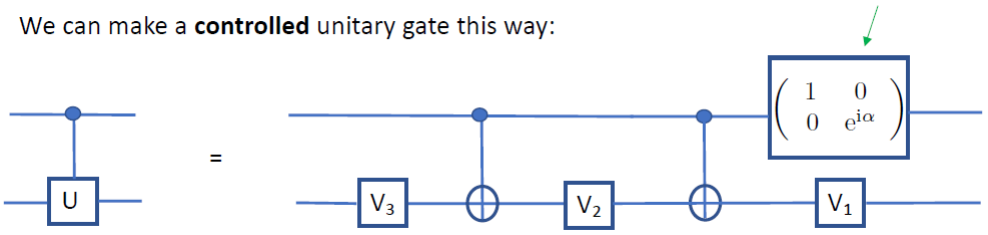
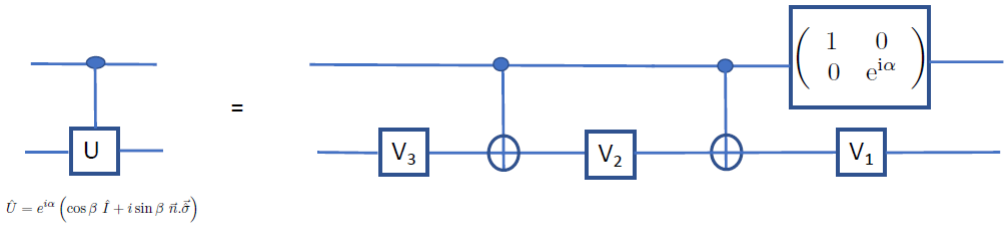


Figure: From "Quantum gates & circuits", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.



Our two requirements (constraints if you'd like) are, first (for when CNOT gates are both "off")

$$\widehat{V}_3\widehat{V}_2\widehat{V}_1 = \widehat{I}$$

and

$$\widehat{V}_3\widehat{X}\widehat{V}_2\widehat{X}\widehat{V}_1 e^{i\alpha} = \widehat{U}$$

The first condition is satisfied simply by choosing

$$\widehat{V}_2 = \widehat{V}_3^{\dagger}\widehat{V}_1^{\dagger}$$

and for the second we need

$$\widehat{V}_3\widehat{X}\widehat{V}_2\widehat{X}\widehat{V}_1 e^{i\alpha} = \widehat{U} = e^{i\alpha}(\cos(\beta)\widehat{I} + i\sin(\beta)\vec{n}\cdot\vec{\widehat{\sigma}})$$

with $\widehat{X} = \widehat{\sigma}_x$, so

$$(\widehat{V}_3\widehat{\sigma}_x\widehat{V}_3^\dagger)(\widehat{V}_1^\dagger\widehat{\sigma}_x\widehat{V}_1) = \cos(\beta)\widehat{I} + i\sin(\beta)\vec{n}\cdot\vec{\widehat{\sigma}}$$

and the unitary operators enclosing $\widehat{\sigma}_X$ produce rotations of this Pauli operator, so we have

$$\widehat{\sigma}_X \to \widehat{V}_3\widehat{\sigma}_x\widehat{V}_3^\dagger = \vec{b}\cdot\vec{\widehat{\sigma}}$$
$$\widehat{\sigma}_X \to \widehat{V}_1^\dagger\widehat{\sigma}_x\widehat{V}_1 = \vec{c}\cdot\vec{\widehat{\sigma}}$$

with $\vec{b}$ and $\vec{c}$ any unit vectors we desire. If we use the identity below,

$$(\vec{b}\cdot\vec{\widehat{\sigma}})(\vec{c}\cdot\vec{\widehat{\sigma}}) = (\vec{b}\cdot\vec{c})\widehat{I} + i(\vec{b}\times\vec{c})\cdot\vec{\widehat{\sigma}}$$

and if we choose $\vec{b}, \vec{c}$ s.t.

$$\vec{b}\cdot\vec{c} = \cos\beta$$
$$\vec{b}\times\vec{c} = \sin(\beta)\vec{n}$$

then we will get the state we desire.

.

Example 5. Toffoli gate:

This is a three-qubit gate. It is also known as the controlled-controlled-NOT (CCNOT). Two of the qubits are control ones, the remaining one being the target qubit.

This gate leaves the state of the control qubits unchanged, but flips the state of the target ($|0\rangle \leftrightarrow |1\rangle$) if BOTH control qubits are in the state $|1\rangle$. It can be represented by the following operator:

$$\widehat{U}_{\text{Toffoli}}\,|A\rangle\otimes|B\rangle\otimes|C\rangle \to |A\rangle\otimes|B\rangle\otimes\left|C\oplus(\underbrace{A\cdot B}_{\text{AND}})\right\rangle,$$

where $\oplus$ is the "addition modulo 2", and $A\cdot B$ stands for "A and B". If you're not familiar with the concept of a sum modulo 2, here is how it behaves:

$$0\oplus 0 = 0$$

$$0\oplus 1 = 1\oplus 0 = 1$$

$$1\oplus 1 = 0$$

so it almost behaves like the usual sum + (in base 2) except that in the last case when one would reach 2 it goes back to zero instead, which is the remainder of the division of $(1+1)/2 = 1+0$.

Remark 6. The Toffoli CCNOT gate can be made from 2 CNOT gates and 3 single qubit gates (look at the diagram below)

Toffoli gate

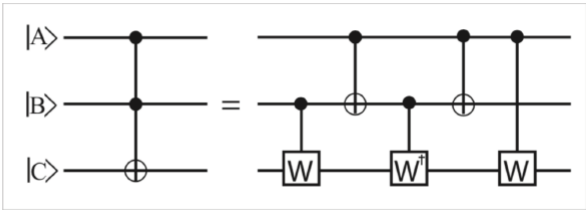


Figure: From "Quantum gates & circuits", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

where the controlled W-gate performs the unitary transformation

$$\widehat{W} = \frac{1-i}{2}(\widehat{I} + i\widehat{\sigma}_x), \quad \text{if the control qubit is in state } |1\rangle.$$

Notice that

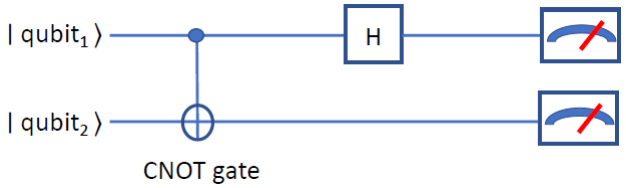
$$\widehat{W}^\dagger = \frac{1+i}{2}(\widehat{I} - i\widehat{\sigma}_x)$$

$$\widehat{W}^2 = \widehat{\sigma}_x$$

Since any controlled-unitary gate can be made from CNOT and single qubit gates, therefore the Toffoli gate can be made by means of just CNOT and single qubit gates.

1.4. A circuit for Bell measurements

We have presented the circuit below in the context of Bell's theorem:



where the last part in the circuit represents a measurement in the computational basis $|0\rangle, |1\rangle$, and the H in the middle represents a Hadamard gate.

Fact 7. *We remark that the possible outcomes of the measurements are:* $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

An interesting fact about the CNOT and Hadamard gates (involved in the circuit abovementioned) is that their inverse gates are themselves! Namely,

$$\widehat{U}_{CNOT} = \widehat{U}^\dagger_{CNOT} = \widehat{U}^{-1}_{CNOT}$$

$$\widehat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \widehat{H}^\dagger = \widehat{H}^{-1}$$

We will use this fact (together with the remark above regarding possible measurement outcomes) to understand the combined action of our gates, since it's easier to see their effect backwards (given the remark about inverses):

$$|00\rangle \to \widehat{H}\otimes\widehat{I}\,|00\rangle = \frac{|00\rangle+|10\rangle}{\sqrt{2}} \to \widehat{U}_{CNOT}\frac{|00\rangle+|10\rangle}{\sqrt{2}} = \frac{|00\rangle+|11\rangle}{\sqrt{2}} = \left|\Phi^{+}\right\rangle$$

$$|01\rangle \to \widehat{H}\otimes\widehat{I}\,|01\rangle = \frac{|01\rangle+|11\rangle}{\sqrt{2}} \to \widehat{U}_{CNOT}\frac{|01\rangle+|11\rangle}{\sqrt{2}} = \frac{|01\rangle+|10\rangle}{\sqrt{2}} = \left|\Psi^{+}\right\rangle$$

$$|10\rangle \to \widehat{H}\otimes\widehat{I}\,|10\rangle = \frac{|00\rangle-|10\rangle}{\sqrt{2}} \to \widehat{U}_{CNOT}\frac{|00\rangle-|10\rangle}{\sqrt{2}} = \frac{|00\rangle-|11\rangle}{\sqrt{2}} = \left|\Phi^{-}\right\rangle$$

$$|11\rangle \to \widehat{H}\otimes\widehat{I}\,|11\rangle = \frac{|01\rangle-|11\rangle}{\sqrt{2}} \to \widehat{U}_{CNOT}\frac{|01\rangle-|11\rangle}{\sqrt{2}} = \frac{|01\rangle-|10\rangle}{\sqrt{2}} = \left|\Psi^{-}\right\rangle$$

1.5. DiVincenzo Criteria (1996)

This stands for the necessary conditions to build a quantum computer, enumerated below.

1. A well-defined extendible and stable qubit array.
2. The ability to prepare this qubit array in a suitable starting state (say such as all qubits in the state $|0\rangle$).
3. A good isolation from the environment (that is, long coherence times).
4. The ability to perform a universal set of gate operations (single-qubit rotations and CNOT operations, or any chosen pair of qubits, which requires addresability if individual qubits).
5. The ability to perform something close to ideal Von Neumann neasurements on each of the qubits.

1.6. Alternate approaches to quantum computing

So far we have presented the "gate-based paradigm" of quantum computing: we usually start with an array of qubits prepared in a simple state ($|0\rangle\otimes|0\rangle\otimes|0\rangle\cdots$) and then we perform single-/multi- qubit operations step by step, by means of gates. Noticeable the multi-qubit gates generate entanglement between qubits. At the end there will be a measurement stage.

On the other hand, there are alternative approaches, that we will mention below for completeness:

- Cluster states [Proposed by R. Raussendorf, D.E. Browne and H.J. Briegel in "Measurement-based quantum computation on cluster states" Phys. Rev. A 68, 022312 (2003)]: These states are highly entangled multi-qubit ones, forming the starting point of the computation. A sequence of single-qubit measurement follows, and after that single-qubit unitary transformations (dependent on the preceding measurement results) follow after.

- Quantum Annealing / Adiabatic quantum computation: Idea is that the solution to our problem is given by the ground state of a particular Hamiltonian. System starts in the ground state of a simpler Hamiltonian, and then the parameters of the Hamiltonian are slowly changed, until it evolves into the Hamiltonian we desire. As long as the evolution is slow enough (adiabatic), the adiabatic theorem guarantees that the system will always remain in the ground state. One competitor following this line is D-Wave, for example, as in the work illustrated below.

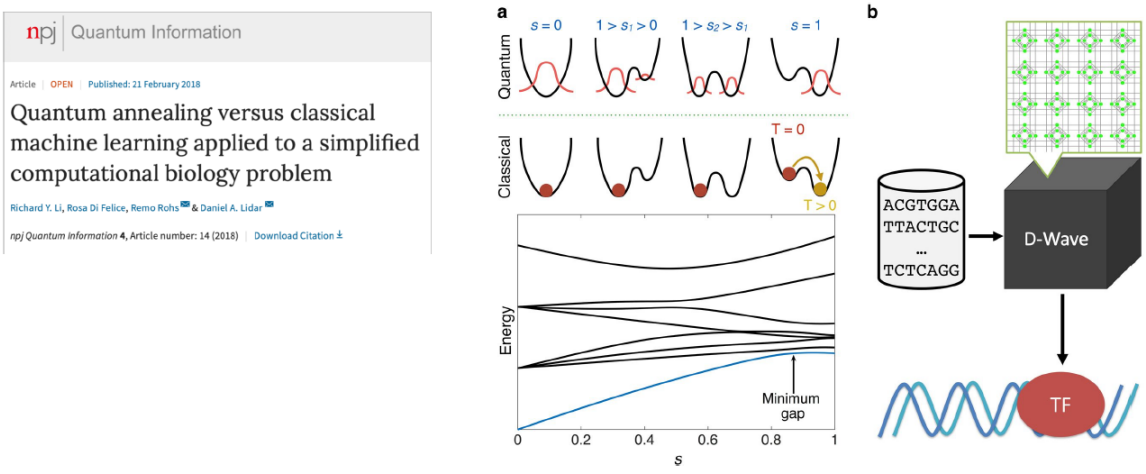


Illustration of the principles and purpose of this work. **a** Top: Quantum versus classical adiabatic annealing processes. With quantum annealing there is the possibility for the system state (red) to tunnel through a changing barrier (black) and arrive at the ground state; for classical annealing, the system must rely on thermal fluctuations (temperature $T > 0$) to overcome any energy barriers. Bottom: Typical spectrum of instantaneous energy eigenvalues during adiabatic quantum optimization. The ground state energy at $s = 0$ has a significant gap to the next energy level. The speed at which the optimization can take place depends on the size of the minimum gap. **b** Using simplified data sets of a small number of sequences derived from actual binding affinity experiments, we use D-Wave, a commercially available quantum annealer, to classify and rank binding affinity preferences of a TF to DNA

Figure: From "Quantum gates & circuits", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

1.6.1. Quantum Annealing and the Traveling Salesman Problem (TSP)

You might be already familiar with the TSP, but if not, here's a simple description of it (in the context of ice-cream trucks):

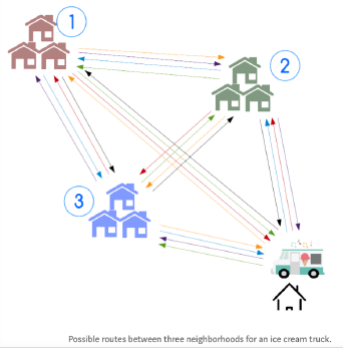


Figure: From https://medium.com/@quantum_wa/quantum-annealing-cdb129e96601

Problem 8. Traveling Salesman Problem [TSP]: Find the shortest route for the ice-cream truck in the diagram above.

With only 3 places to deliver, the number of possible routes to calculate is for this particular case only 3!=6.

These 6 possible routes are:

$$1 \to 2 \to 3$$

$$1 \to 3 \to 2$$

$$2 \to 1 \to 3$$

$$2 \to 3 \to 1$$

$$3 \to 1 \to 2$$

$$3 \to 2 \to 1$$

If there are 5 places/towns to deliver, then the # of routes is 5!=120. Likewise, for N towns then the number of routes is N!, but you should notice that this number grows quite large even for a small N=20, since

$$20! = 2432902008176640000$$

If you look at the link of the figure, you will see that there's an equivalence between the TSP and the problem of anti-ferromagnetic Ising model (you can map one problem into another), if you make the interaction between spins dependent on the distance between towns. That is, a greater distance implies higher energy. The optimal solution should have the lowest energy among all. Clearly this is an optimization problem, which is actually non-trivial (classically, techniques attempting to solve it are for example Simulated Annealing, google the seminal Nature paper).

1.7. Quantum Simulations

Problem 9. We desire to simulate a quantum system on a classical computer. If there are N qubits (say N interacting spins), there are then 2^N possible states. Therefore, keeping track of the state vector requires storing 2^N probability amplitudes, specifically $2(2^N - 1)$ independent real numbers, because

$$\underbrace{2\times}_{\text{complex }\#}\ (2^N - \underbrace{1}_{\text{normaliz.}}) = 2^{N+1} - 2.$$

The short answer is that the numbers above depends exponentially in N. In general, a Hamiltonian will be represented by a $2^N \times 2^N$ Hermitian matrix (specified by 2^{2N} independent real numbers, if you think about Hermiticity constraints). Since we will use the Hamiltonian to evolve the state vector, we will require then an exponential number of computational steps. Therefore, the actual time that will be required to calculate the time evolution of the state vector is exponential in N as well.

Solution 10. In order to avoid these difficulties (inherent to attemps of simulating quantum systems by classical computers), we'd better use another quantum system (easier to control and manipulate) to simulate the one of interest brought up first!

Remark 11. This was the original remark of Feynman when he proposed quantum computers to better simulate quantum systems in his famous & seminal paper "Simulating physics with computers", Int J Theor Phys 21, 467–488 (1982).

Example 12. Ultra-cold neutral atoms in an optical lattice can be used to simulate electrons in a metal. So we model the latter quantum system with the former one.

References

[1] "Quantum gates & circuits", by Prof. Duncan O'Dell, Introduction to Quantum Information course, McMaster University, 2019.

[2] Quantum Information, by Stephen M. Barnett (Oxford University Press, ISBN 978-0-19-852763-3).

[3] Quantum Annealing, by Alba Cervera-Lierta, QWA & Quantic group. https://medium.com/@quantum_wa/quantum-annealing-cdb129e96601

[4] Feynman, R.P. Simulating physics with computers. Int J Theor Phys 21, 467–488 (1982). https://doi.org/10.1007/BF02650179