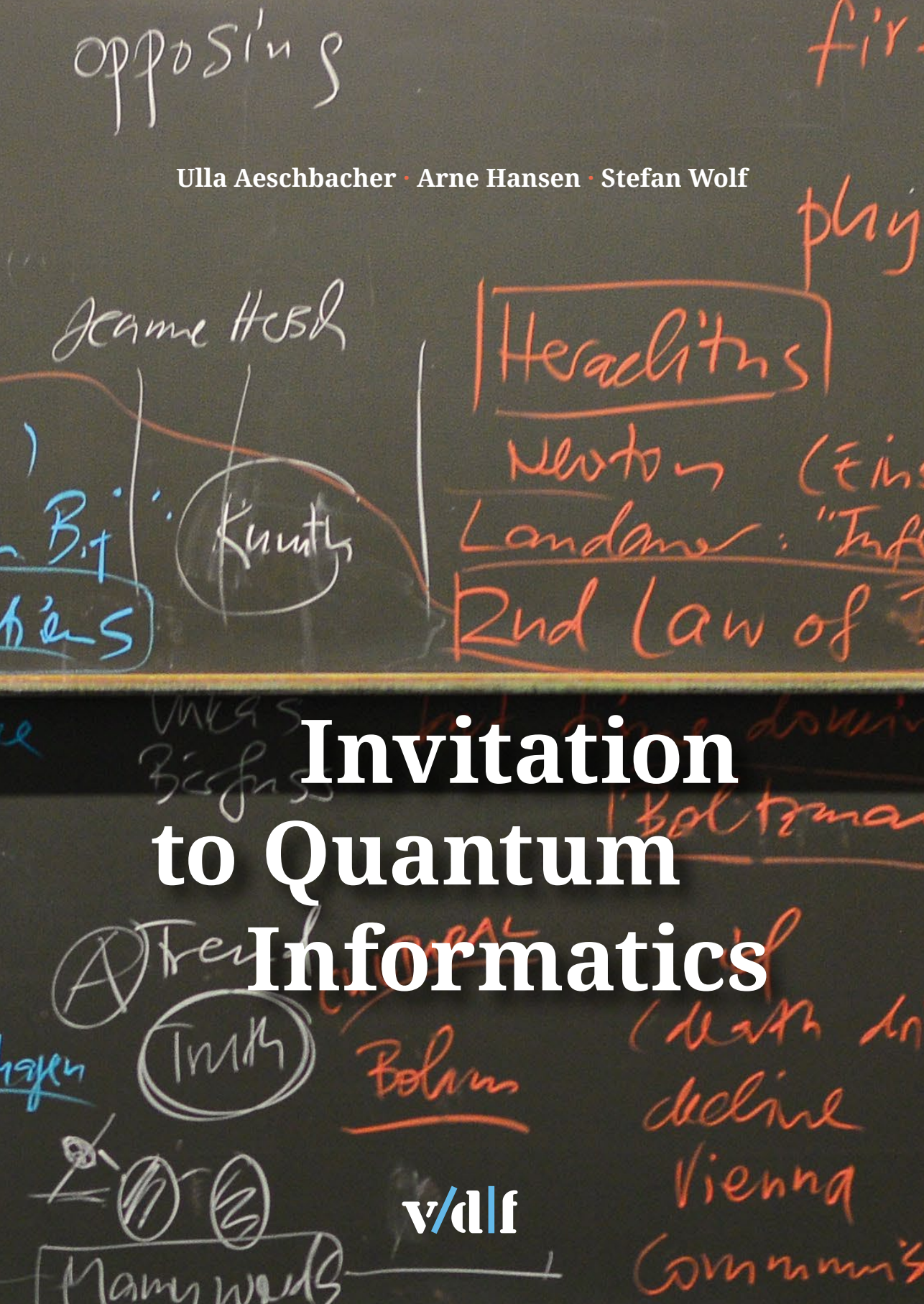


Ulla Aeschbacher · Arne Hansen · Stefan Wolf

Invitation to Quantum Informatics

v/dlf

Ulla Aeschbacher · Arne Hansen · Stefan Wolf

Invitation to Quantum Informatics

v/d|f

Bibliographic Information published by Die Deutsche Nationalbibliothek
Die Deutsche Nationalbibliothek lists this publication in the Internet at
http://dnb.dnb.de.

ISBN 978-3-7281-3988-7 (Printausgabe)

Download open access:
ISBN 978-3-7281-3989-4 / DOI 10.3218/3989-4

www.vdf.ethz.ch
verlag@vdf.ethz.ch

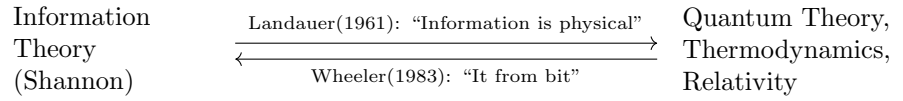
Contents

Chapter 1

What Is Quantum Informatics?

1.1 Information & Physics

Physics and *Information (Theory)* are two different sciences, *i.e.*, two thinking traditions both rooted in their respective histories, coined by their own methods, personalities, and established truths. The present text belongs to the (postmodern) tradition of considering, establishing, discussing, and analyzing the connections between physics and information. Of these connections, there are essentially two natures: On the one hand, experience, observation, and physical discourse are in the form of information: *John Archibald Wheeler* compressed this fact to the slogan "It from Bit." On the other hand, information representation, processing, and transmission are, ultimately, *physical* processes; as *Rolf Landauer* put it: "Information is Physical."



This text starts from the latter insight and discusses consequences thereof both of limiting (thermodynamics) and enabling (quantum theory) character of physical law for information treatment. On occasion, a glimpse is offered at the possibility of obtaining new insights into natural law when the informational point of view is chosen. The text culminates in *Peter Shor*'s algorithm, born out of a surprising and breathtaking marriage between quantum physics and number theory. (*Claus Hepp* called the algorithm the "most fascinating result in theoretical physics of its decade," due to its internal conceptual beauty,

not its "real-world" application that is, at this point, potential, unclear, and debated.)

Concretely, Landauer's slogan means that the representation of a bit of information, if this bit is to "exist," must be physical. This implementation can be realized by a switch, a current in a metal wire going one way as opposed to the other, the position of a single gas molecule in a container, the polarization of a photon, or by the electron of a hydrogen atom in its ground as opposed to first excited state. The latter example is interesting since it illustrates that *digitalization* in fact comes very naturally with quantization (*e.g.*, of energy levels) whereas in classical physics, it has to be enforced in some way. Later in the text, however, we will see that quantum physics allows for another kind of "world between zero and one" that could more accurately be enabled by the possibility of "being zero and one at the same time (at least to some extent)."

If we follow that thought through, we realize that physical laws thus can have direct consequences for information processing. Although that is true in principle, it seems that the nature of these consequences probably depends strongly on the specific choice of the information's physical representation. Or — to turn that thought around — are those physical laws that have consequences that are *independent* of that representation (beyond the fact that there *is* such a representation) perhaps laws that are rather logical-informational than "physical" in the strict sense?

The second law of thermodynamics states that, in a closed system, *entropy* does not decrease (with overwhelming probability). What is entropy? A first, rough answer is that it is some kind of measure for *disorder*. A precise answer is harder; *John von Neumann* was quoted as saying "if you want to win any discussion, just say 'entropy' and you will be on the safe side, because nobody really knows what entropy is." It has also been said that *Claude Shannon*, the founder of information theory, followed von Neumann's advice when he chose the name "entropy" for the central quantity of his theory.

A remarkable feature of the second law is its *time asymmetry*, which contrasts the time symmetry of most physical laws and processes. Exceptions are some elementary-particle reactions and, more importantly for us, *measurements*. Related notions thus would be *past* and *future*: the arrow of time.

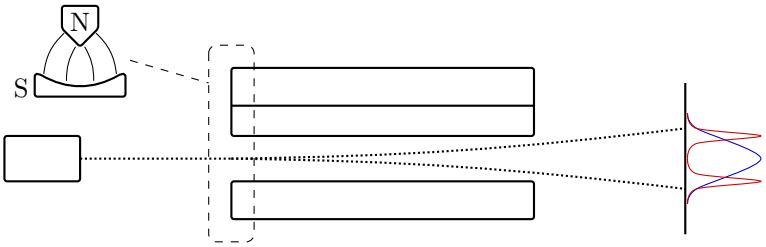
Whereas entropy (disorder) may be hard to define in general, it is clear in some cases: Given that N binary memory cells contain a "random" content (an equally problematic notion, in fact) and are then all erased (put to 0), the entropy in the set of memory cells drops.

1.2 The Stern/Gerlach Experiment

1.2.1 Independent Measurements?

The Stern/Gerlach experiment — proposed by Otto Stern in 1921 [16] and carried out by Walther Gerlach in 1922 [8] — was not the first in the history of quantum theory, but one of the most important ones to understand the structure and properties of the basic building block of quantum information processing, the *quantum bit (Qbit)*. In particular, the question was what *classical* information we can get on such a Qbit, and how.

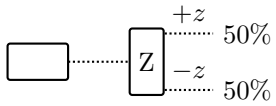
In the experiment, Stern and Gerlach measure a certain quantity, the *magnetic dipole moment*, of silver atoms by sending a stream of such atoms, exiting an oven, through a inhomogeneous magnetic field. Each atom is then deflected from the path proportionally to its dipole in the direction of the magnets. If we imagine that the moments of the atoms point in random directions (and have, perhaps, constant length or even varying length within some range or according to some distribution), then the classical expectation is that the deflection pattern reaches a maximum in the middle (no deflection) and then symmetrically, monotonically, and continuously decreases on the sides. This is, however, not what was observed: There is no detection in (not even close to) the middle, but rather two sharp peaks at equal distances from that middle.



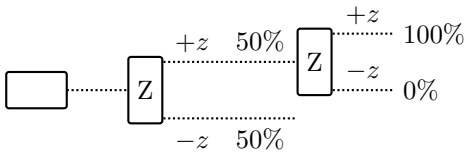
This "quantization" is one of the characteristic features of quantum theory — to which it owes its name, too — and motivated assigning the quantity a new name in that context: *spin*.[1]

[1]The following anecdote was reported concerning this experiment: Initially, Gerlach did not see any detection of the screen supposed to register the trajectories of the silver atoms. Desperately, he handed the blind plates to Stern, who gave it a look to; during that, some of the air Stern was breathing out hit the plates. The thing is that the cigars Stern used to smoke (heavily) contained a lot of sulfur; they were cheap cigars, as physics researchers were not well paid at the time, it seems. In the end, the sulfur initiated the reaction necessary to see the detections on the screen, and the experiment succeeded. The story is sometimes taken to support the argument that also social and economic factors (Stern's salary and the quality of his cigars, etc.) have to be considered in the context of physical experiments dismantling "objective" reality.

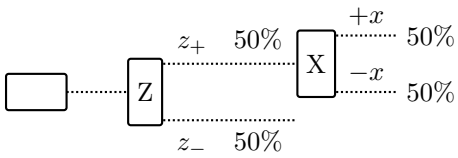
In the case of a single Stern/Gerlach measurement, say, in the Z-direction, two identical rays result. Let us call the rays by the properties they correspond to, i.e., $Z-$ and $Z+$.



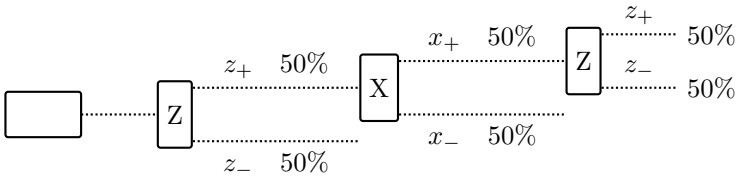
If the same measurement is repeated on, say, only the $Z+$ ray, then all atoms are again deflected in the $+$ direction. In this sense, the Z-spin property looks classical: It is stable with respect to repeated measurements.



When the magnet is rotated into the spatial X direction (also perpendicular to the flying direction Y of the atoms), then a $50-50$ distribution arises. This is not surprising due to the geometrical symmetry of the situation. It is equally unsurprising that the same is observed when the second measurement (the one in X direction) is carried out *after* a Z measurement from which only the $Z+$ counts are carried over to the next experiments: It means that the two properties, "Z-spin" and "X-spin," look *independent*.



The most fascinating outcome results when the two types of measurement are combined as follows: First, a Z measurement, whereby only $Z+$ counts are transferred to the next magnet, an X measurement. If subsequently, another Z measurement is performed, then half the particles show $Z-$ spin, although we took only $Z+$ states after the first measurement. This is puzzling and questions both our interpretations above: The *stability* as well as the *independence* of the properties in question.



Interlude

The *stability of a measurement result* is not so surprising: Popper regards scientifically interesting physical effects to be defined by being reproducible by anyone and at anytime, provided that one builds the same experimental setup.[a] The "scientific method" crucially relies on being able to enquire about equivalent questions and then expect the same answer. There must at least exist some conditions under which this is possible. This does, however, not imply that this is possible under all conditions as one might hope coming from classical mechanics.

[a] "Der wissenschaftlich belangvolle physikalische Effekt kann ja geradezu dadurch definiert werden, daß er sich regelmäßig und von jedem reproduzieren läßt, der die Versuchsanordnung nach Vorschrift aufbaut." [14, §I.8]

1.2.2 Superposition

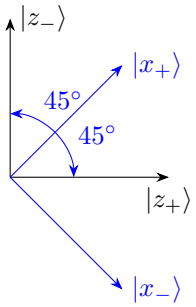
The statistics found within the Stern/Gerlach experiment were surprising for *single* particles. They would not have been surprising if we had dealt with waves. Imagine a polarizing filter in a beam of light. Then measuring z_+ can be considered to correspond to passing a polarizing filter of a certain orientation; measuring z_- corresponds to passing a polarizing filter rotated by 90°. If the beam initially is unpolarized, then the probability of passing such a polarizing filter—or the ratio of the intensity before and after the filter—is 50%. Measuring with a filter rotated by 45° with respect to the z_+ filter would correspond to x_+. Then the intensities measured in a sequence of filter would fit the probabilities in the Stern/Gerlach experiment.

The essential property of waves is that they can be linearly combined. Quantum mechanical states have the same property: They are elements in a vector space. But their length does not relate to wave amplitudes; instead, they serve to derive probability distributions. Thus, linearly combined states have to be normalized. The z_+ filter then corresponds to asking whether the silver atom is in a z_+ state, denoted by $|z_+\rangle$. If the silver atom does not go up, i.e., it is not in a state $|z_+\rangle$, then it goes down, i.e., it is in a state $|z_-\rangle$, orthogonal to $|z_-\rangle$. So, the question whether the silver atom is in the state $|z_+\rangle$ and the question whether the silver atom is in the state $|z_-\rangle$ are complementary to one another. In fact, they can also be regarded as two different answers to the same question, i.e., the Z measurement.

If, after a Z measurement, we perform an X measurement, then we want to know whether the silver atom is in a state $|x_+\rangle$ or in a state $|x_-\rangle$. Both are equal superpositions,

$$|x_+\rangle = \frac{1}{\sqrt{2}}|z_+\rangle + \frac{1}{\sqrt{2}}|z_-\rangle \qquad |x_-\rangle = \frac{1}{\sqrt{2}}|z_+\rangle - \frac{1}{\sqrt{2}}|z_-\rangle.$$

No matter whether we had obtained z_+ or z_- in the Z measurement, the X measurement yields one of both results with equal probability.[2] Also in the inverse order: A Z measurement after an X measurement yields the same uniform distribution—independent of any measurements before the X measurement.



Interlude

So, a phenomenological perspective, i.e., from a comparison of probability distributions, suggests the superposition of states in quantum mechanics. Quantum mechanics attains an essential property of wave mechanics, even though there are no more coupled system, with a description in, e.g., classical mechanics. The states are then more abstracts entities. They are no longer directly observable properties of a system, but rather tools to determine probability distributions for measurement results.[a]

[a] *Grete Hermann* describes quantum states as "new symbols that express the mutual dependency of the determinability of different measurements." [10]

1.3 Quantum Key Distribution

Previously we have seen: The condition for measuring *with certainty* the same value in two consecutive measurements with the same measurement basis, e.g., in two consecutive Z measurements, is that there is no intermediary measurement in another bases. In other words: The interactions of a system with its environment, within, say, a measurement, become traceable. This allows us to detect an eavesdropper in a cryptographic key agreement protocol. In 1984, Gilles Brassard and Charles Bennett developed the first application of quantum mechanics for cryptographic purposes with such a key agreement protocol [2].

Let us assume that Eve and Bob can exchange quantum mechanical systems. Then they can establish a secret key as follows: Alice chooses at random

[2] The details of how to derive probabilities from states will be given later.

a measurement, either Z or X, and measures a quantum system, e.g., a silver atom, in that basis. She then sends that system to Bob, who also chooses at random between a Z and an X measurement, and performs the measurement on that system. If the bases that Alice and Bob choose coïncide, then the results of their measurements are the same—unless there has been an eavesdropper, Eve, measuring the system during its transmission from Alice to Bob in a basis different from Alice's and Bob's. Alice and Bob do *not* agree beforehand on a basis. Instead, they repeatedly measure quantum systems in randomly chosen bases. So, Eve can merely guess Alice's choice of measurement. If Alice's choice was really random then, in some cases, Eve guesses wrongly and, therefore, disturbs the system. Alice and Bob can trace that disturbance as follows: Alice repeatedly chooses random measurement and sends the states after the measurement over to Bob, e.g.,

Alice's measurement	×	+	+	×	+	×	×	+	×
result	0	0	1	0	1	1	0	0	1

.

Bob also chooses his bases at random and measures the state:

Alice's measurement	×	+	+	×	+	×	×	+	×
result	0	**0**	**1**	0	1	**1**	0	**0**	1
Bob's measurement	+	+	+	+	×	×	+	+	+
result	1	**0**	**1**	0	0	**1**	1	**0**	1

.

Where their bases agree, their measurement result are the same, if there is no eavesdropper. So, Alice and Bob communicate over an authenticated channel the positions in the above sequence where they do agree. Now, to ensure that there has been no eavesdropper, they finally choose randomly some of the positions where their results should be the same and compare whether they actually are. If Eve had been intercepting and measuring the states, then the results should differ in about 1/4 of the cases. If Alice and Bob find that their results are the same in (almost) all cases, then they can use the remaining, unpublished measurement result (where their measurement bases agree) as a secret key.

1.4 The Double-Slit Experiment

If one shines light onto a double slit, an *interference pattern* appears on a screen behind the double slit. What happens, however, if one sends *single* electrons or *single* photons onto the double slit? Intuitively one would expect two peaks, corresponding to each of the slits. Instead, if one measures the position of the electrons or photons on the screen for many repetitions of the experiment, an interference pattern emerges.