**Zeitschrift:** Helvetica Physica Acta

**Band:** 42 (1969)

**Heft:** 3

**Artikel:** Impossibility of quantum mechanics in a Hilbert space over a finite field

**Autor:** Eckmann, J.-P. / Zabey, Ph.Ch.

**DOI:** https://doi.org/10.5169/seals-114075

# Impossibility of Quantum Mechanics in a Hilbert Space over a Finite Field

by **J.-P. Eckmann** and **Ph. Ch. Zabey**
Institute of Theoretical Physics, University of Geneva

(12. VIII. 68)

*Abstract.* In this paper, we show that the lattice of propositions of a quantum mechanical system cannot be represented as subspaces of Hilbert Space with coefficients from a finite field.

The only exceptions are the two dimensional lattices, for which the restriction on the field is only that it may not be of characteristic 2.

## 1. The Structure of Irreducible Proposition Systems[1])

According to the axiomatic of JAUCH and PIRON, the set of all "yes-no" experiments of a physical system is an irreducible proposition system $L$, i.e. a partially ordered set with the following properties,

(i) *It is a complete lattice:* every family $\{a_i\}_i$ of elements of $L$ admits a greatest lower bound $\Lambda_i\, a_i$ and a least upper bound $V_i\, a_i$.

(ii) *It is orthocomplemented:* there exists a mapping $a \in L \mapsto a' \in L$ which is involutive ($a'' = a$), decreasing ($a \leqslant b$ implies $b' \leqslant a'$) and such that $a \; V \; a' = I$, where $I = V_{a \in L}\, a$ is the greatest element of $L$, we define also $0 = I' = \Lambda_{a \in L}\, a$ as the least element of $L$.

(iii) *It is weakly modular:* if $a \leqslant b$, then $a = (a \; V \; b') \; \Lambda \; b$.

(iv) *It is atomic:* every non zero element admits an atom as lower bound; by atom we mean a non zero element $p$ such that $0 < x \leqslant p$ implies $x = p$.

(v) *It satisfies the covering law:* if $p$ is an atom and $a$ any element such that $a \; \Lambda \; p = 0$, then $(p \; V \; a') \; \Lambda \; a$ is an atom.

(vi) *It is irreducible:* for every pair of atoms $(p, q)$, there exists a third atom $r$ such that $p \; V \; q = p \; V \; r = q \; V \; r$.

The following example ensures the compatibility of these properties; denote by $L(V)$ the set of all biorthogonal manifolds of a euclidian or of a unitary space $V$. The order in $L(V)$ is given by the inclusion, and the orthocomplementation by taking the orthogonal complement. This set $L(V)$ is a genuine irreducible proposition system.

Conversely, one shows that an irreducible proposition system $L$ can be realized by the set of all biorthogonal manifolds of a vector space $V$ over some field $F$, the

---

[1]) This section is mostly an extract from: J. M. JAUCH, *Foundations of Quantum Mechanics* (Chapter 8).

orthocomplementation defining on $F$ an involutive antiautomorphism $\alpha \mapsto \bar{\alpha}$[2]) and on $V$ a scalar product, that is a non degenerate sesquilinear hermitian form $S: V \times V \to F$. The field $F$ over which $V$ is defined is, up to an isomorphism, determined by the algebraic structure of $L$. Usually one takes for $F$ either the field $\mathcal{R}$ of real numbers, or the field $\mathcal{C}$ of complex numbers, or the field $\mathcal{H}$ of quaternionic numbers; each of these is a complete valuated field.

The purpose of this paper is the study of finite dimensional vector spaces over finite fields; such fields are necessarily complete, for they admit only the trivial valuation $|0| = 0$ and $|\alpha| = 1$ for $\alpha \neq 0$.

*Remarks:*

1. In the following we shall say subspace for biorthogonal manifold.
2. We can use a graphical representation for lattices; a point will figure an element, and a "climbing" line an order relation.

$$\begin{array}{c} \circ\ a \\ | \\ \circ\ b \end{array} \quad \text{means } a \leq b.$$

In the case of a lattice $L(V)$, it will be sufficent to give all possible inclusions between any subspace and a subspace of immediately higher dimension.

## 2. Finite Fields

Let $F$ be a finite field, and $u$ its unit element. A theorem by WEDDERBURN[3]) states that $F$ is always abelian. The prime field of $F$, defined as the subfield generated by $u$, is isomorphic to the field $\mathcal{Z}_p$, where $p$ is a prime number called the characteristic of the field ($\mathcal{Z}_p$ stands for the field of integers modulo $p$). Thus $F$ is a finite extension of $\mathcal{Z}_p$ with dimension $d$ over $\mathcal{Z}_p$, and its order is $p^d$. One knows that to each power $p^d$ of a prime number $p$ ($d \geqslant 1$) there exists, up to an isomorphism, a unique field with $p^d$ elements; one usually writes it as $GF(p, d)$[4]); its multiplicative group is cyclic of order $p^d - 1$.

Under an automorphism of $F = GF(p, d)$, $u$ and therefore the elements of the prime field $\mathcal{Z}_p$ are invariant. The group $\mathrm{Aut}(F)$ of automorphisms is cyclic of order $d$; each automorphism of $F$ can be written as:

$$\alpha \in F \mapsto \alpha^{(p^\delta)} \in F \quad (\delta = 0, 1, 2, \ldots, d-1)\,.$$

The group $\mathrm{Aut}(F)$ has as generating element the automorphism $\alpha \mapsto \alpha^p$.

$F$ has a non trivial involution (that is an automorphism of order 2) if and if only $d$ is even. Evidently, in that case the automorphism

$$\alpha \in F \mapsto \alpha^{(p^c)} \in F \quad (c = d/2)$$

is a non trivial involution, and there is no other one possible. We write:

$$\bar{\alpha} = \alpha^{(p^c)}.$$

We say that $GF(p, 2c)$ is of *complex type* whereas $GF(p, 2c + 1)$ is called of *real type*, and we shall use the terms and notations commonly adopted, except for $|\alpha|^2 = \alpha\,\bar{\alpha}$, because a finite field admits only the trivial valuation.

---

[2]) $\bar{\bar{\alpha}} = \alpha$; $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$; $\overline{\alpha\beta} = \bar{\beta}\,\bar{\alpha}$.

[3]) See E. ARTIN, *Geometric Algebra* (Chapter 1, section 8).

[4]) $GF$ = Galois Field.

### 3. Lattices $L(p, d, n)$

Let $V$ be a vector space of dimension $n$ over the field $GF(p, d)$. Let $L(p, d, n)$ denote the lattice of all subspaces of $V$. We intend to calculate the number $N_k(p, d, n)$ of subspaces of dimension $k$ $(0 \leqslant k \leqslant n)$ and the number $L_{k,k+1}(p, d, n)$ of subspaces of dimension $k+1$ containing one of the subspaces of dimension $k$ $(0 \leqslant k < n)$.

First note that each subspace of dimension $k$ has $p^{dk}$ elements, or in other words $p^{dk} - 1$ non zero vectors.

We calculate the number $T_k(p, d, n)$ of ordered $k$-frames[5]) of $V$; evidently, $T_n(p, d, n)$ denotes the number of ordered bases of $V$. We proceed by the construction of an ordered $k$-frame. There are $p^{dn} - 1$ possibilities to choose the first vector of the frame; afterwards there remain $p^{dn} - p^d$ vectors in $V$ which are linearly independent from the first chosen, that is there are $p^{dn} - p^d$ possibilities to choose the second vector of the frame; there remain $p^{dn} - p^{2d}$ vectors linearly independent from the first two chosen, and out of these we choose the third one; and so on. It follows that

$$T_k(p, d, n) = \pi_{i=0}^{k-1} (p^{dn} - p^{di}) \qquad (0 < k \leqslant n) . \tag{3.1}$$

We define $T_0(p, d, n) = 1$. As there are $T_k(p, d, k)$ ordered bases for one $k$-dimensional subspace, $N_k(p, d, n)$ is given by

$$N_k(p, d, n) = \frac{T_k(p, d, n)}{T_k(p, d, k)} . \tag{3.2}$$

$L_{k,k+1}(p, d, n)$ is calculated as follows. A subspace of dimension $k+1$ contains $N_k(p, d, k+1)$ subspaces of dimension $k$. As there are $N_{k+1}(p, d, n)$ subspaces of dimension $k+1$, the total number of inclusions is $N_k(p, d, k+1)\, N_{k+1}(p, d, n)$. Now there are $N_k(p, d, n)$ subspaces of dimension $k$, and as each of them is included in the same number $L_{k,k+1}(p, d, n)$ of subspaces of dimension $k+1$, we have

$$L_{k,k+1}(p, d, n) = \frac{N_k(p, d, k+1) N_{k+1}(p, d, n)}{N_k(p, d, n)} = T_1 (p, d, n-k) . \tag{3.3}$$

The formulas (3.2) and (3.3) characterize completely the structure of the lattice $L(p, d, n)$.

The next problem discussed in this paper is the following: describe all possible orthocomplementations of $L(p, d, n)$. This description is possible for all such lattices and is given by the following theorem.

**Theorem:** Let $L(p, d, n)$ be defined as before. An orthocomplementation is possible only if $p \neq 2$ and $n = 2$, for each value of $d$. In this case, there are

$$\frac{(2\,q)\,!}{q\,!\; 2^q} \qquad (2\,q = p^d + 1)$$

different ways to realize the orthocomplementation.

The proof of this theorem is divided into three parts:

1st part: (section 4) $n = 2$.

2nd part: (section 5) $n > 2$ and $d$ odd (real fields).

3rd part: (section 6) $n > 2$ and $d$ even (complex fields).

---

[5]) A *k-frame* is a set of $k$ linearly independent vectors; a *basis* is a total frame.

## 4. Two-dimensional Vector Spaces

In a two-dimensional vector space, an orthocomplementation is an involutive permutation of the 1-dimensional subspaces which leaves no element invariant. Evidently, the number of 1-dimensional subspaces must be even for such an involution to exist. But we know that:

$$N_1(p, d, 2) = \frac{p^{2d}-1}{p^d-1} = p^d + 1 .$$

If $p = 2$, $p^d + 1$ is odd and there is no orthocomplementation.

If $p \neq 2$, $p$ is odd and thus $p^d + 1$ is even, and there are orthocomplementations. Their number is equal to the number of pairings of $2q = p^d + 1$ elements, this number is:

$$(2q-1)(2q-3)\ldots 3 \cdot 1 = \frac{(2q)!}{2^q q!} .$$

We summarize:

**Lemma:** A lattice $L(2, d, 2)$ admits no orthocomplementation. A lattice $L(p, d, 2)$, with $p \neq 2$, admits

$$\frac{(2q)!}{2^q q!} \qquad (2q = p^d + 1)$$

orthocomplementations.

## 5. Vector Spaces over Real Fields, with Dimension $n > 2$

The fields $GF(p, 2c + 1)$ have no non trivial involution. It follows that an orthocomplementation must be induced by some *bilinear form* $B : V \times V \to F = GF(p, 2c + 1)$. Before giving the main lemma of this second part, let us recall a few general notions.

A *quadratic space* is a pair $(V, B)$ consisting of a vector space $V$ and a bilinear symmetric form $B : V \times V \to F$. Let $x$ be any vector of a quadratic space. It is said to be *isotropic* when $B(x, x) = 0$; note that the zero vector is always isotropic. The space $V$ itself is said to be *isotropic* when it contains a non zero isotropic vector.

*Remark:* In a euclidian or in a unitary space, the scalar product, being non degenerate, does not admit any non zero isotropic vector; thus such a space is never isotropic.

An orthocomplementation of $L(p, 2c + 1, n)$ is induced by a bilinear symmetric form bringing $V$ into a non isotropic space. We recall now the following important result: "A quadratic space over a finite field is isotropic if its dimension is greater than or equal to 3"[6]). As a corollary we have now our main lemma.

**Lemma:** A lattice $L(p, 2c + 1, n)$, with $n \geqslant 3$, admits no orthocomplementation.

## 6. Vector Spaces over Complex Fields, with Dimension $n > 2$

These fields have a non trivial involution $\alpha \mapsto \bar{\alpha}$. So we have two possibilities to choose the form defining the orthocomplementation.

[6]) See O. T. O'Meara, *Introduction to Quadratic Forms* (Section 62).

A. *The involution is the identity*

Then, again, the orthocomplementation is induced by a bilinear symmetric form, and the arguments of the previous section apply; there is no such form.

B. *The involution is not trivial*

In this case the orthocomplementation is induced by a sesquilinear hermitian form $S : V \times V \to F$, which, in a suitable basis $(e_1, \ldots, e_n)$, is diagonal:

$$S(x, y) = \Sigma_{i=1}^{n} \alpha_i \bar{x}_i y_i$$

where $x = \Sigma_i x_i e_i$ and $y = \Sigma_i y_i e_i$. The hermiticity of $S$ implies $\bar{\alpha}_i = \alpha_i$ for all $i$'s. Let $\tilde{V}$ denote a vector space of same dimension as $V$ but defined over the subfield of $F$ of the elements invariant under the involution $\alpha \mapsto \bar{\alpha}$; this subfield, denoted by $\tilde{F}$, corresponds to the real axis of $F$. $\tilde{V}$ may be identified to a subset of $V$. The restriction of $S$ to $\tilde{V}$ defines a bilinear symmetric form $B : \tilde{V} \times \tilde{V} \to \tilde{F}$:

$$x, y \in \tilde{V} \Rightarrow B(x, y) = S(x, y) .$$

As $\dim \tilde{V} = \dim V \geqslant 3$, $\tilde{V}$ is isotropic for $B$, after the arguments of the previous section, and hence $V$ is also isotropic for $S$.

We have therefore proved our last lemma.

**Lemma:** A lattice $L(p, 2c, n)$, with $n \geqslant 3$, admits no orthocomplementation.

The three lemmas of the sections 4, 5 and 6 are sufficient to prove the theorem we stated in section 3.

## 7. Concluding Remarks and Acknowledgements

Only a lattice $L(p, d, 2)$, with $p \neq 2$, admits at least one orthocomplementation. Such a lattice can always be imbedded in the proposition system of the polarization states of a photon, i.e. the lattice of subspaces of the unitary space $\mathbb{C}^2$.

We would like to thank Prof. J. M. Jauch for having suggested this problem and for his advice during its solution.

This research was partially supported by the National Science Foundation.

## Bibliography

E. Artin, *Geometric Algebra* (Interscience Publ., New York, 1957).
R. Baer, *Linear Algebra and Projective Geometry* (Academic Press, 1952).
J. M. Jauch, *Foundations of Quantum Mechanics* (Addison-Wesley, 1968).
O. T. O'Meara, *Introduction to Quadratic Forms* (Springer-Verlag, 1963).
B. L. van der Waerden, *Algebra* (Springer-Verlag, 1966).