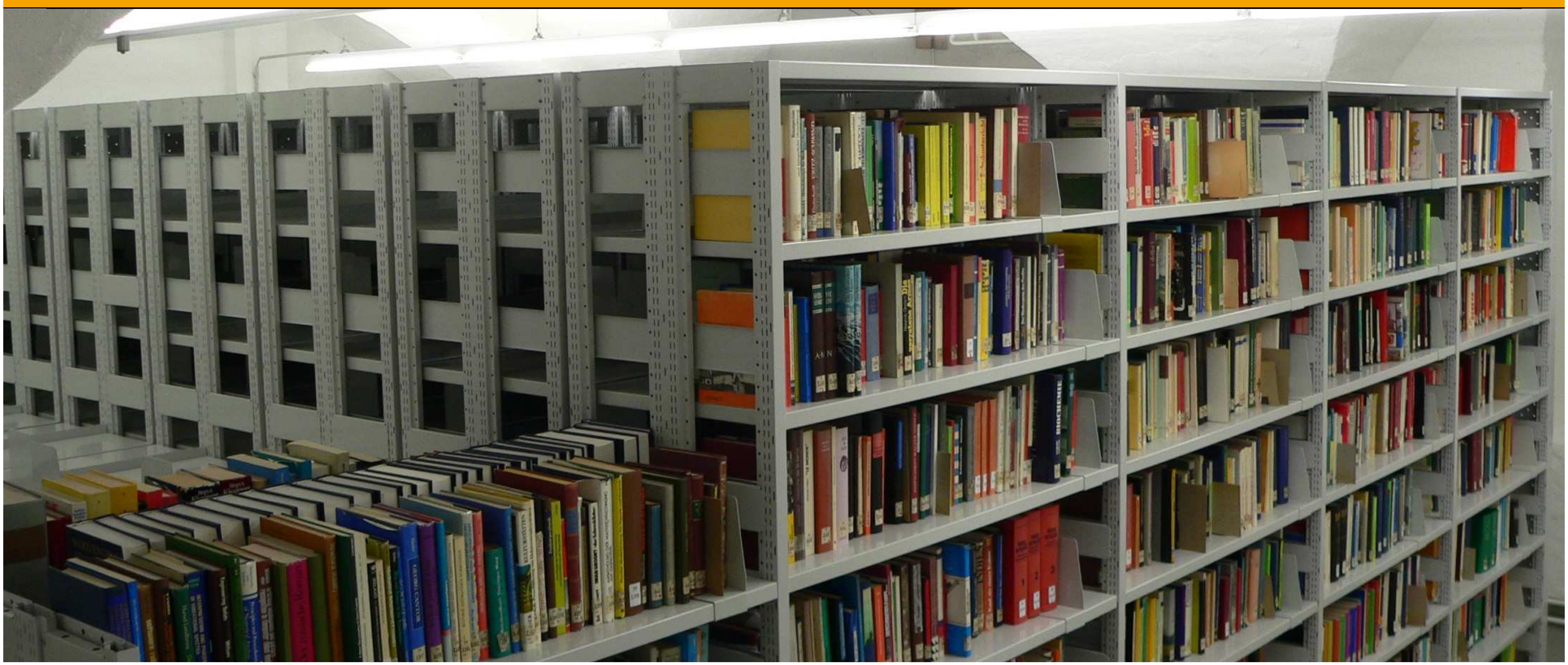
Christian Herrmann

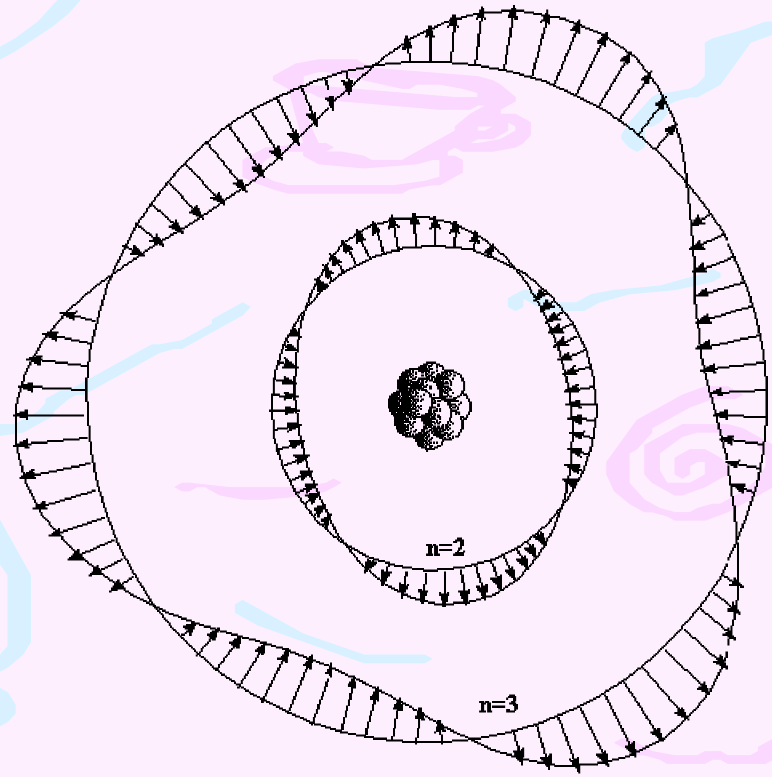
Computational Complexity of Quantum Satisfiability

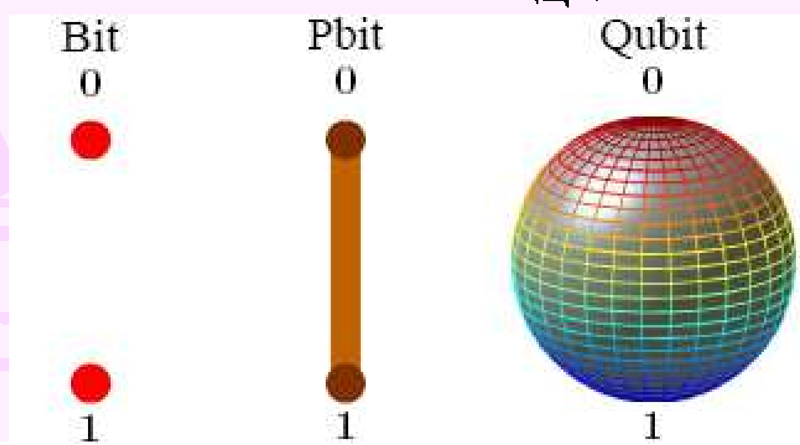
TECHNISCHE UNIVERSITÄT DARMSTADT

Martin Ziegler



fascinating Quantum Mechanics

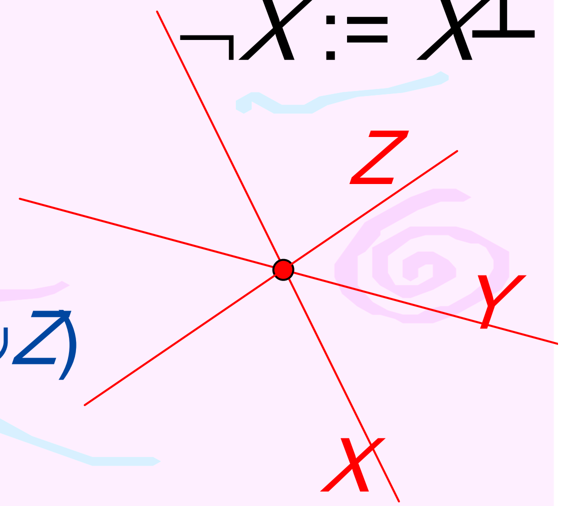




Geometric Quantum Logic

For field $\mathbb{F}\subseteq\mathbb{C}$ and $d\in\mathbb{N}$, consider the family $\mathrm{Gr}(\mathbb{F}^d)$ of all subspaces of $\mathbb{F}^d$, equipped with

$X\wedge Y := X\cap Y$, $\quad X\vee Y := X+Y$, $\quad \neg X := X^{\perp}$



$(S,\cap,\cup,\setminus)$ Boolean logic:

- –de Morgan $\quad S\setminus(X\cup Y) = (S\setminus X)\cap(S\setminus Y)$
- –distributive $\quad X\cup(Y\cap Z) = (X\cup Y)\cap(X\cup Z)$
- –self-dual; neutral elements $\emptyset$ and S

$(\mathrm{Gr}(\mathbb{F}^d),\wedge,\vee,\neg)$: de Morgan, self-dual, neutral $\{0\},\mathbb{F}^d$

- –but not distributive in dimensions ≥2. $\quad$ 1*D Boolean*
- –Instead **modular law**: $\quad X\subseteq Z \Rightarrow X\vee(Y\wedge Z) = (X\vee Y)\wedge Z$
- –Neumann'55, Birkhoff'67, Kalmbach'83, Beran'85, …

Overview: 2D, 3D, fixed-dim., indefinite finite-dim.

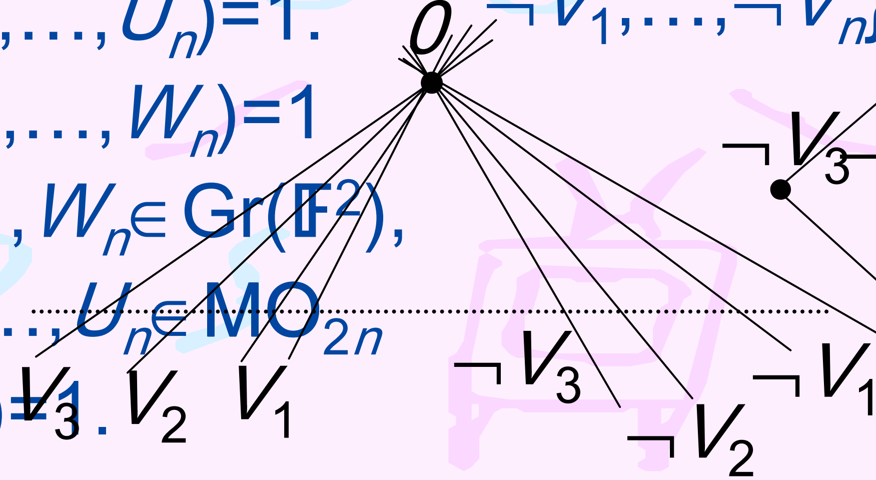
2D Quantum Logic $\mathrm{Gr}(\mathbb{F}^2)$

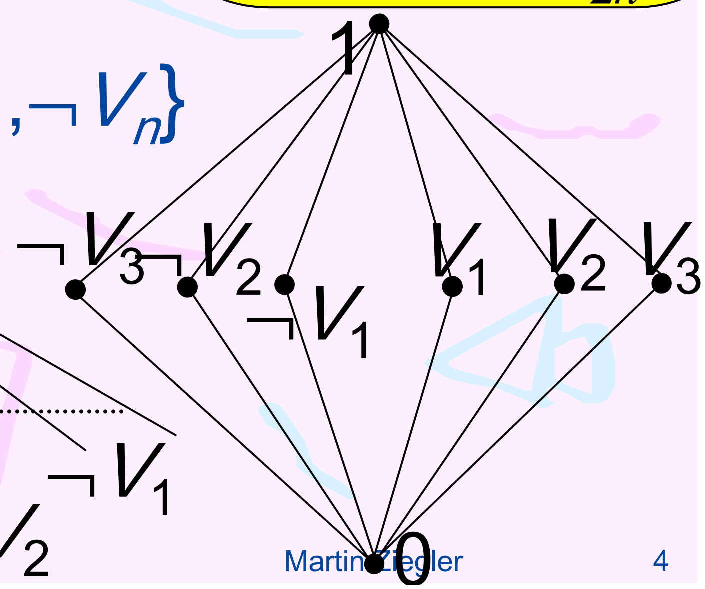
Def: Formula f is (strongly) satisfiable if $f(U_1,\ldots,U_n)=1$ for some subspaces $U_1,\ldots,U_n \subseteq \mathbb{F}^d$; weakly satisfiable if $f() \neq 0$

Theorem: 2D satisfiabiliy is $\mathcal{NP}$-complete (as in 1D)

Proof, "$\in \mathcal{NP}$": Given formula $f(X_1,\ldots,X_n)$,
prepare 1D subspaces (=lines) $V_1,\ldots,V_n$
with $0 = V_i \wedge V_j = \neg V_i \wedge V_j = \neg V_i \wedge \neg V_j \quad \forall i \neq j$
Then guess $U_1,\ldots,U_n \in \{0,1, V_1,\ldots,V_n, \neg V_1,\ldots,\neg V_n\}$
and verify $f(U_1,\ldots,U_n)=1$.

$\{0,1,V_1,\ldots,V_n, \neg V_1,\ldots,\neg V_n\}$ is a ortholattice called $\mathbf{MO}_{2n}$





Lemma: If $f(W_1,\ldots,W_n)=1$
for some $W_1,\ldots,W_n \in \mathrm{Gr}(\mathbb{F}^2)$,
there exist $U_1,\ldots,U_n \in \mathbf{MO}_{2n}$
with $f(U_1,\ldots,U_n)=1$.

2D Quantum Logic Gr($\mathbb{F}^2$)

Def: Formula f is (strongly) satisfiable if $f(U_1,\ldots,U_n)=1$ for some subspaces $U_1,\ldots,U_n \subseteq \mathbb{F}^d$; weakly satisfiable if $f() \neq 0$

Theorem: 2D satisfiabiliy is $\mathcal{NP}$-complete (as in 1D)

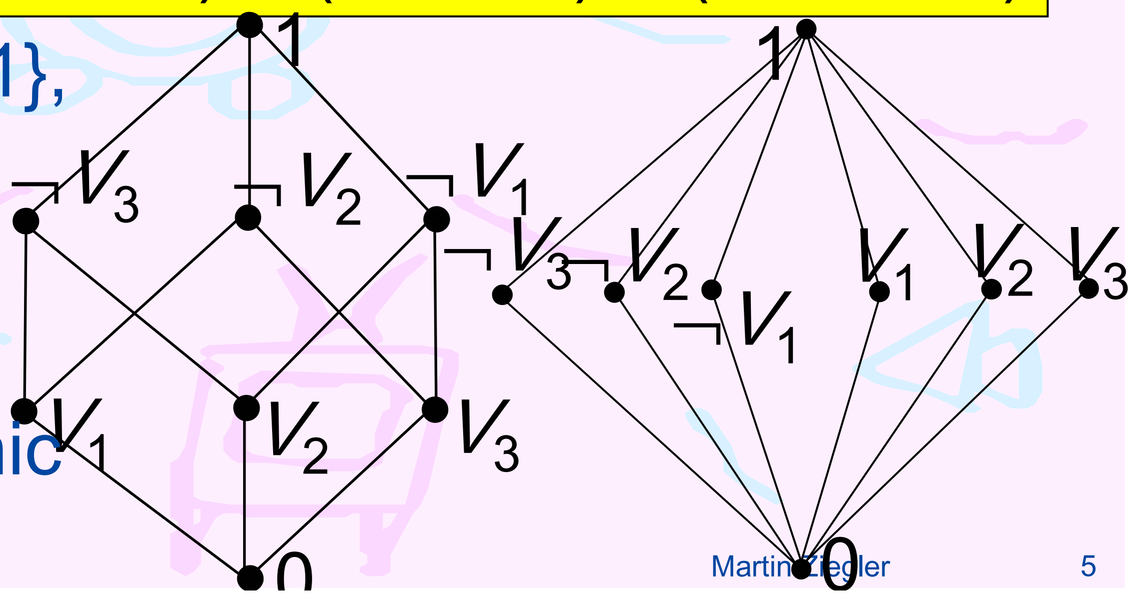
Proof, $\mathcal{NP}$-hardness: Given formula $f(X_1,\ldots,X_n)$, consider $g(X_1,\ldots,X_n) := f(X_1,\ldots,X_n) \wedge \bigwedge_{i \neq j} \mathrm{C}(X_i,X_j)$.

works in any dimension!

$$\mathrm{C}(X,Y) := (X \wedge Y) \vee (X \wedge \neg Y) \vee (\neg X \wedge Y) \vee (\neg X \wedge \neg Y)$$

Lemma: a) For $X,Y \in \{0,1\}$, it holds $\mathrm{C}(X,Y)=1$.

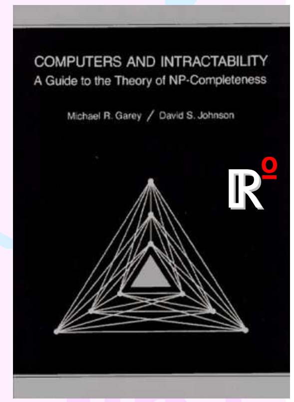
b) If $\mathrm{C}(X_i,X_j)=1 \ \forall i \neq j$, then $X_1,\ldots,X_n$ generate an ortholattice isomorphic to $\{0,1\}^k$ for some $k \leq 2n$.



Turing vs. BSS Machine

Discrete: Turing Machine / Random-Access Machine (TM/RAM)

Input/output: finite sequence of bits $\{0,1\}^*$ or integers $\mathbb{Z}^*$



Each memory cell holds one element of $R=\{0,1\}$ / $R=\mathbb{Z}$

~~`Program' can store finitely many constants from *R*~~

operates on R (for TM: $\vee, \wedge, \neg$; for RAM: $+, -, \times, <$)

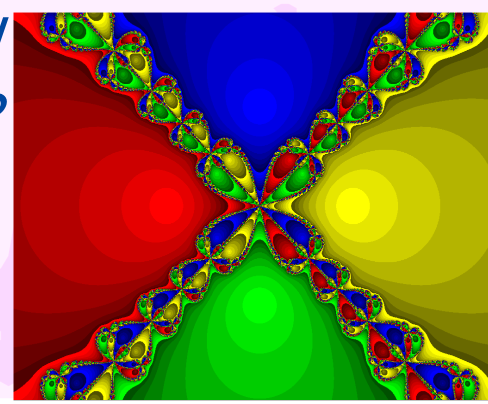
Computation on algebras/structures **[Tucker&Zucker]**, **[Poizat]**

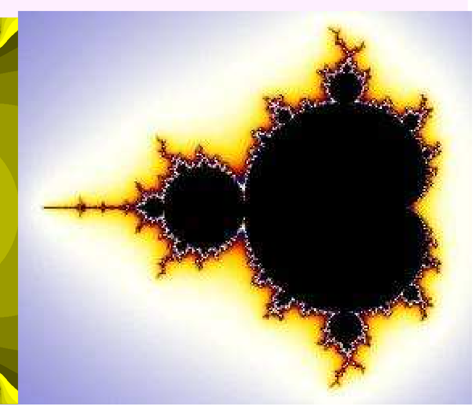
on $\mathbb{R}^* := \bigcup_k \mathbb{R}^k$: Algebra $(\mathbb{R},+,-,\times,\div,<)$ $\rightarrow$ real-RAM, BSS-machine

[Blum&Shub&Smale'89], [Blum&Cucker&Shub&Smale'98]

$\mathcal{P}_{\mathbb{R}}^{\circ} \subseteq \mathcal{NP}_{\mathbb{R}}^{\circ} \subseteq \mathcal{EXP}_{\mathbb{R}}^{\circ}$ (Tarski Quantifier Elimination) strict?

$\mathcal{NP}_{\mathbb{R}}^{\circ}$-complete: *Does a given real int. polynom.system have a real root?*





$\mathbb{H} \subseteq \mathbb{R}^*$ real Halting problem

Undecidable, too: Mandelbrot Set, Newton starting points

Fixed-dim Satisfiability in **PSPACE**

QSAT($\mathbb{C}^d$), d fixed: Given a formula f over $\wedge,\vee,\neg,X_1,\ldots X_n$:
nondet. polytime **BSS**-machine can 'guess' $A_1,\ldots,A_n \in \mathbb{C}^{d\times d}$
and evaluate f(range A_1,…,range A_n) using Gauß Elim:
in $\mathcal{NP}^\circ_\mathbb{R}$

Need real/imag to calculate $\neg A \cong A^+$ in $\langle \underline{x}, \underline{y} \rangle$

Thm [Canny'88, Renegar'92] efficient real quantifier elim:
Turing machine can decide in $\mathcal{PSPACE}$ whether a given system of multivariate integer polynomials has a real root

complete for $\mathcal{NP}^\circ_\mathbb{R} \subseteq \mathcal{PSPACE}$

No 'better' (e.g. in $\mathcal{PH}$) algorithm known to-date!
(Allender, Bürgisser, Kjeldgaard-Pedersen, Miltersen'06: $\mathcal{P}^\circ_\mathbb{R} \subseteq \mathcal{CH}$)

Similarly with integer root: undecidable (Matiyasevich'70)

Similarly with rational root: unknown (e.g. Poonen'09)

Similarly with complex root: $co\mathcal{RP}^{\mathcal{NP}}$ mod **GRH** (Koiran'96)

3D: von Staudt Ring Operations

Let $X(r) := \{ (z,x,rx) : x,z \in \mathbb{F} \} \in \mathrm{Gr}_2(\mathbb{F}^3)$

and $Y(s) := \{ (sy,x,y) : x,y \in \mathbb{F} \} \in \mathrm{Gr}_2(\mathbb{F}^3)$,

and $Z(t) := \{ (tz,z,y) : y,z \in \mathbb{F} \} \in \mathrm{Gr}_2(\mathbb{F}^3)$, $r,s,t \in \mathbb{F}$.

Then $(X(r) \wedge Y(s)) \vee \neg X(0) = Z(s \bullet r)$.

relative to $X(1)$

Similarly expressible: addition, subtr., cmplex conjugation:

To given polynomial $p \in \mathbb{Z}[X_1,\ldots,X_n,X_1^*,\ldots,X_n^*]$,
TM can in polynomial time construct
a quantum logic formula $f_p(Y_1,\ldots,Y_N)$ such that
f_p is satisfiable over $\mathrm{Gr}(\mathbb{F}^3)$ iff p admits a root in $\mathbb{F}$.

e.g. X^2-2 or X^2+1

a) Generally need irrational/complex subspace to satisfy f.

b) 3D satisfiability complete for $\mathcal{NP}^\circ_{\mathbb{R}}$

c) d-dim. satisfiability polytime-reducible to 3D case

Dimensional Heredity / Weak versus Strong

So far considered only strong satisfiability: $f(X_1,\ldots,X_n)=1$

Hagge et. al. (2005,'07,'09): For n-variate formula f, write

$\mathrm{maxdim}(f,d) := \max\{\,\dim\big(f(V_1,\ldots,V_n)\big) : V_1,\ldots,V_n \in \mathrm{Gr}(\mathbb{C}^d)\,\}$

Lemma: a) $\mathrm{maxdim}(f,d+k) \geq \mathrm{maxdim}(f,d) + \mathrm{maxdim}(f,k)$

b) $\mathrm{maxdim}\big(f(\underline{X})\vee g(\underline{Y}),d\big)=\min\big(d,\mathrm{maxdim}(f,d)+\mathrm{maxdim}(g,d)\big)$

c) The *restriction* $f|_g(\underline{X},\underline{Y})$ of formulas $f(\underline{X})$ and $g(\underline{Y})$

has $\mathrm{maxdim}(f|_g,d)=\mathrm{maxdim}(f,\mathrm{maxdim}(g,d))$

d) There exists a formula ψ_d with $\mathrm{maxdim}(\psi_d,m)=\lfloor m/d\rfloor$.

- f *weakly* satisfiable in dimension d $\Rightarrow$ also in dim $d+1$
- f *strongly* satisfiable in dim d and k $\Rightarrow$ also in dim $d+k$
- $\neg C(X,Y)$ *strongly* satisfiable precisely in even dimensions

In dimension d:

$f(\underline{X})$ weakly satisfiable iff $f(\underline{X}_1)\vee\ldots\vee f(\underline{X}_d)$ strongly satisfiable

And f strongly satisfiable iff $\psi_d|_f$ weakly satisfiable

$C(X,Y) := (X \wedge \neg Y) \vee (\neg X \wedge Y)$

weak $\preccurlyeq_p$ strong | strong $\preccurlyeq_p$ weak | d-dim $\preccurlyeq_p$ $(d+k)$-dim

Indefinite Finite Dimensions

Definition: f weakly/strongly satisfiable over $\mathrm{Gr}(\mathbb{F}^*)$
iff weakly/strongly satisfiable over $\mathrm{Gr}(\mathbb{F}^d)$ <u>for some $d \in \mathbb{N}$</u>.

f weakly satisfiable in dim $d \Rightarrow$ also in every dim $\geq d$.

Sophisticated induction on syntactic length of formula f:
f weakly satisfiable in <u>some</u> dim $\Rightarrow$ also in dim $= |f|^2$

Theorem: a) weak satisfiability over $\mathrm{Gr}(\mathbb{C}^*)$ is in $\mathcal{NP}^\circ_{\mathbb{R}}$

b) strong satisfiability over $\mathrm{Gr}(\mathbb{C}^*)$ is $\mathcal{NP}^\circ_{\mathbb{R}}$–hard

decidable? semi-decidable!

There are formulas of length $O(n)$ strongly satisfiable in dimension 2^n but not in lower dimensions.

Summary and Conclusion

Boolean logic:
- ubiquitous, natural, classical
- computational complexity well-established
- including many famous open problems

Quantum logic in dimension *d*
- generalizes Boolean logic (d=1)
- multivalued, de Morgan, but not distributive
- motivated by physics, nice geometric intuition

Thank you!

1D + 2D quantum satisfiability: $\mathcal{NP}$-complete
d-dim satisfiability (d≥3): complete for $\mathcal{NP}^{\circ}_{\mathbb{R}}$
d-dim strong satisfiability $\equiv_p$ d-dim weak satisfiability
*In*definite finite dimension: strong satisfiability decidable?

Quantified Quantum Propositional Logic

f satisfiable in $\mathrm{Gr}(\mathbb{F}^*)$ $\Leftrightarrow$ $\exists d\in\mathbb{N}\ \exists \underline{X}\in \mathrm{Gr}(\mathbb{F}^d)$: $f(\underline{X})=1$ $\quad\Sigma_1$

Σ_k: $\exists d\in\mathbb{N}\ \exists \underline{X}^{(1)}\in \mathrm{Gr}(\mathbb{F}^d)\ \forall \underline{X}^{(2)}\ \exists \underline{X}^{(3)}\ldots\Theta \underline{X}^{(k)}$: $f(\underline{X}^{(1)},\ldots,\underline{X}^{(k)})=1$

Π_k: $\forall d\in\mathbb{N}\ \forall \underline{X}^{(1)}\in \mathrm{Gr}(\mathbb{F}^d)\ \exists \underline{X}^{(2)}\ \ldots\ \Theta \underline{X}^{(k)}$: $f(\underline{X}^{(1)},\ldots,\underline{X}^{(k)})=1$

Similarly with "$f(\ldots)\neq 0$" instead "$=1$": weak Σ_k/ Π_k formula.
Complement of a Σ_k formula is a weak Π_k formula!

Example: $X\in\{0,1\}$ $\Leftrightarrow$ $\forall Y$: $C(X,Y)=1$. $\quad\Pi_1$

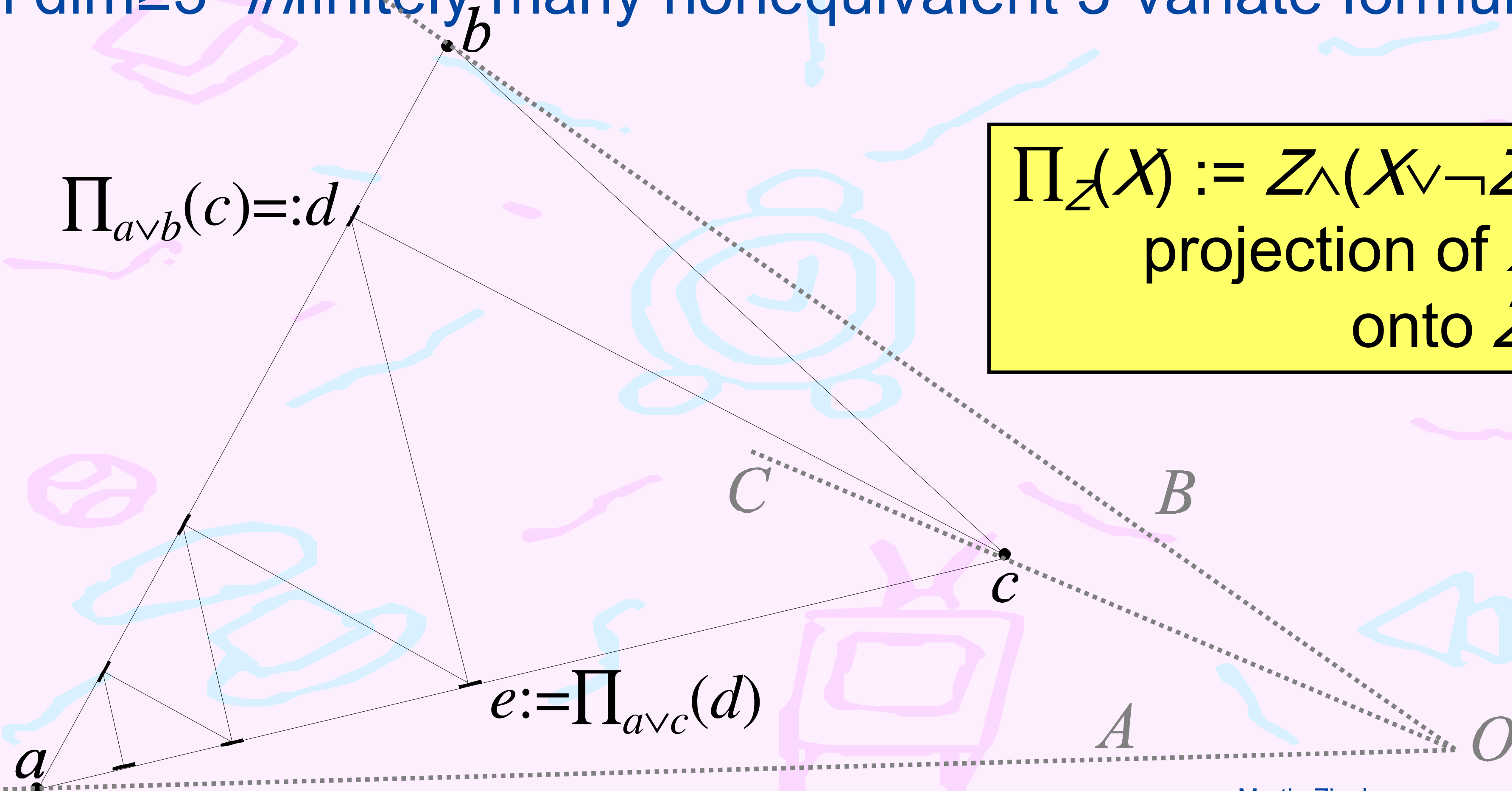
No $f(X,\underline{Y})$ has, over $\mathrm{Gr}(\mathbb{F}^*)$, "$X\in\{0,1\}$ $\Leftrightarrow$ $\exists\underline{Y}$: $f(X,\underline{Y})=1$"

Theorem: The restricted word problem for finite-semigroups (undecidable according to Gurevich) can be encoded as a Σ_4-formula over $\mathrm{Gr}(\mathbb{F}^*)$.

higher-dim. Quantum Logic

Haviar, Konôpka, Wegener ('97) / Herrmann & Z.: cmp.1D: 2^{2^n}
in dim=2, $2^{2^{\Theta(n\cdot\log n)}}$ nonequivalent n-variate formulas

In dim≥3 *in*finitely many nonequivalent 3-variate formulas



$\prod_Z(X) := Z\wedge(X\vee\neg Z)$ projection of X onto Z.

Quantum Logic as a mathematical model of QM

	Classical Physics	
states in a system	elements s of some set S	
physical observables	functions $f: S \rightarrow \mathbb{R}$	s
measurement result	$f(s)$	
'property' (0/1 –observable)	funct. $f: S \rightarrow \{0,1\}$ $\leftrightarrow$ subset X of S	
conj./disj./neg of prop.s X, Y	$X \cap Y$, $X \cup Y$, $S \setminus X$ $X \wedge Y$, $X \vee Y$, $\neg X$