On the equational theory of projection lattices of finite von Neumann factors
Christian Herrmann
on joint work with Luca Giudici [10] and Martin Ziegler [12]
Jardafest, Praha July 22, 2010

0. MODULAR (ORTHO) LATTICES

We consider modular lattices (shortly MLs) - we write \(a + b\) for joins and \(ab\) for meets - and modular ortholattices (shortly MOLs), a subject started by Birkhoff and von Neumann [1]. These have constants 0 and 1 and a unary fundamental operation \(x \mapsto x'\) which is an involution and, moreover, an orthocomplementation
\[x'' = x, \quad x \leq y \Rightarrow y' \leq x'; \quad x \oplus x' = 1,\]
The principal examples are the lattices \(L(M)\) of all submodules of some \(R\)-module \(M\) and the lattices
\[L(V, \Phi) = \{X, X^\perp \mid X \in L(V), \dim X < \infty\}, \quad X \mapsto X^\perp\]
where \((V, \Phi)\) is an inner product space. Considering lattice identities \(\forall \mathbf{x} f(\mathbf{x}) = g(\mathbf{x})\), we may assume that \(f(\mathbf{x}) \leq g(\mathbf{x})\) holds in all lattices. In MOLs it suffices to consider identities of the form \(\forall \mathbf{x} t(\mathbf{x}) = 0\) - put \(t = gf'\).

1. IDENTITIES IN THE ATOMIC CASE

**Proposition 1.1.** If \(L\) is an atomistic ML or MOL, then \(L \models \forall \mathbf{x} f(\mathbf{x}) = g(\mathbf{x})\) if and only if \([0, u] \models \forall \mathbf{x}, f(\mathbf{x}) = g(\mathbf{x})\) for all interval subalgebras \([0, u]\) where \(\dim u\) is at most the number of occurrences of variables in \(f\) and \(g\), together.

Here, in the case of MOLs, \([0, u]\) is endowed with the orthocomplement \(x^u = x'u\).

**Lemma 1.2.** In an atomistic ML, if \(h(\mathbf{x})\) is a lattice term with unique occurrence of variables, and if \(p \leq h(\mathbf{x})\) for some atom \(p\), then there is a substitution by atoms such that \(p \leq h(\mathbf{q})\).

**Proof.** By induction. If \(p \leq h_1(\mathbf{a}_1) + h_2(\mathbf{a}_2)\) then there are \(p_i \leq h_i(\mathbf{a}_i)\) such that \(p \leq p_1 + p_2\) - this is, in essence, the Theorem on Joins in projective spaces. By inductive hypothesis we have \(p_i \leq h_i(\mathbf{q}_i)\) for some substitutions by atoms. \(\square\)
Proof. Prop.1. In the lattice case, assume \( f(\overline{a}) < g(\overline{a}) \). Then there is \( p \leq g(\overline{a}) \), \( p \nleq f(\overline{a}) \). Consider \( h(\overline{a}) \) with unique occurrence and substitution \( h(\overline{a}) = g(\overline{a}) \). Then by the Lemma there is a substitution by atoms such that \( p \leq h(\overline{a}) \). Collect all \( q \) associated with the same \( a \) into the join \( c \leq a \) and let \( u \) be the join of all \( c \). Then \( \dim u \) is small as indicated and, by monotonicity of lattice terms, we have \( p \leq g(\overline{a}) \) but \( p \nleq f(\overline{a}) \) in \([0, u]\).

In the MOL case, we replace \( t(\overline{a}) \) by its negation normal form and associate with that a lattice term \( h(\overline{a}, \overline{b}) \) with unique occurrence of variables such that any \( y \) stands for a positive occurrence of some \( x \), any \( z \) for an occurrence of \( x' \). Now, if \( 0 < t(\overline{a}) \), then \( p \leq t(\overline{a}) = h(\overline{a}, \overline{b}) \) where all \( b \)'s are \( a \)'s and all \( c \)'s are \( a' \)'s. By the Lemma, \( p \leq h(\overline{a}, \overline{b}) \) for some substitution by atoms whence \( p \leq t(\overline{d}) \) for some \( d \in [0, u] \), \( u \) the joins of all \( q \)'s and \( r \)'s. Again, \( \dim u \) is bounded as stated. □

Theorem 1.3. Huhn, H., Czédi, Hutchinson. For any division ring \( D \) with prime subfield \( F_p \),

\[ \text{Th}_{eq}(L(V) \mid V a D-vector space) = \text{Th}_{eq}(L(F^n_p) \mid n < \infty) \]

and this equational theory is decidable.

Proof. [7]. \( L(F^n_p) \) is a sublattice of \( L(D^n) \). Any \( L(V_D) \) is a sublattice of \( L(V_{F_p}) \). The latter is atomistic, whence by Prop.1 in the variety generated by the \( L(F^n_p) \). This proves that the varieties coincide. Thus, the set of non-valid identities is recursively enumerable. On the other hand, the quasi-variety generated by the \( L(V_D) \) is recursively axiomatizable - using Mal’cev’s method of axiomatic correspondence. Thus, the equational theory is recursively enumerable, too. A reasonable decision procedure has been provided by Czédi and Hutchinson [3]. □

For MOLs we define the von Neumann variety

\[ \mathcal{N} = \text{HSP}\{L(\mathbb{R}^n) \mid n < \infty\} \]

Theorem 1.4. \( \mathcal{N} = \text{HSP}\{L(\mathbb{C}^n) \mid n < \infty\} \) and \( \text{Th}_{eq}\mathcal{N} \) is decidable.

Here, we consider the canonical real resp. complex scalar products.

Proof. We have the following embeddings \( L(\mathbb{R}^n) \subseteq L(\mathbb{C}^n) \subseteq L(\mathbb{R}^{2n}) \). Also, due to Tarksi [22], \( \text{Th}(\mathbb{R}^n) \) is decidable. Now, apply Prop.1. □

2. Interpretaion of rings via frames

A (von Neumann) \( n \)-frame is a system \( a_{ij} (1 \leq i, j \leq n) \) of constants and relations such that in a lattice \( L(M) \), \( M \) a free \( R \)-module on generators \( e_1, \ldots, e_n \) and \( R \) a ring with unit, these relations are satisfied
for
\[ a_{ii} = e_i R, \quad a_{ij} = a_{ji} = (e_i - e_j)R \]
and, conversely, any system satisfying the relations is, up to isomorphism, this canonical one. In particular, the ring \( R \) can be interpreted into \( L(M) \) via \( r \mapsto (e_1 - e_2^r)R \).

1. For any modular \( L \) with an \( n \)-frame, \( n \geq 4 \), one obtains a ring on \( \{ x \in L \mid x \oplus a_2 = a_1 a_2 \} \). von Neumann [19], mimicking the above.

2. There are terms \( t_{ij}(x) \) such that for an \( a \) in a modular lattice the \( t_{ij}(x) \) form an \( n \)-frame in the interval \( [\prod_{ij} t_{ij}(x), \sum_{ij} t_{ij}(x)] \). Moreover, \( t_{ij}(x) = a_{ij} \) if \( x \) is an \( n \)-frame, already. G. Bergman and A. Huhn [13].

3. For MOLs this extends to orthogonal \( n \)-frames: \( a_{ii} \leq a_{jj} \) for \( i \neq j \) and \( \prod_{ij} a_{ij} = 0 \). R. Mayet and M. Roddy [16].

3. Uniform word problem

A quasi-identity is a first order sentence of the form
\[ \forall \pi. \left( \bigwedge_{i=1}^{n} s_i(\pi) = t_i(\pi) \right) \Rightarrow s(\pi) = t(\pi) \]

Solvability of the uniform word problem for a class \( C \) of algebraic structures means decidability of the set of quasi-identities valid in \( C \). Let \( Q \) denote the quasi-variety generated by \( C \), and \( Q_L \) the class of lattices embedded into reducts of members of \( Q \).

Theorem 3.1. If, for some field \( F \), \( L(F^n) \in Q_L \) for all \( n < \infty \), then the uniform word problem for \( C \) is unsolvable.

Proof. Let \( S \) denote the class of all semigroups, \( F^{n \times n} \) the ring of all \( n \times n \)-matrices over \( F \), and \( F_p \) the prime subfield.

1. \( L(F^n) \cong L(F^{n \times n}) \), the lattice of principal right ideals
2. \( \text{Th}_\forall \{ F^{n \times n} \mid n < \infty \} = \text{Th}_\forall \{ F_p^{n \times n} \mid n < \infty \} = \text{Th}_\forall S_{fin} \) considering multiplicative semigroups Lipshitz [15]
3. \( \text{Th}_\forall S \subseteq \Gamma \subseteq \text{Th}_\forall S_{fin} \) for no recursive \( \Gamma \). Gurevich, Lewis [6].
4. Interpret \( S \to \text{Rings} \to \text{ML} \) via \( F \mapsto F[S] \) and \( R \mapsto L \) via frames

\[ \square \]
4. Restricted word problem

The restricted word problem for \( \mathcal{C} \) considers in each instance a fixed premise \( \bigwedge_{i=1}^n s_i(\pi) = t_i(\pi) \). For a quasi-variety, this amounts to considering a finite presentation. Unsolvability means the existence of some instance with undecidable decision problem.

**Theorem 4.1.** Lipshitz, Hutchinson [15, 14]. If \( L(M) \in \mathcal{Q}_L \) for some free module \( M \) on an infinite basis, then the restricted word problem for \( \mathcal{C} \) is unsolvable - there is a presentation on 5 lattice generators.

Indeed, any finitely presented semigroup can be interpreted into some \( L(M^n) \).

**Theorem 4.2.** Cohn, McIntyre. There is a finitely presented division ring \( D \) with unsolvable word problem.

**Corollary 4.3.** If \( L(D^n) \in \mathcal{Q}_L \) for such \( D \) and some \( n \geq 4 \) then the restricted word problem for \( \mathcal{Q} \) is unsolvable.

**Theorem 4.4.** Roddy [21]. The restricted word problem for MOLs is unsolvable - there is a presentation on 3 generators.

This is based on an intricate construction of a division ring as above admitting a scalar product on some \( D^n - n = 14 \).

5. Undecidable equational theories

**Theorem 5.1.** Freese [4]. The equational theory of all modular lattices is undecidable - 5 and even 4 variables suffice.

The proof is based on the above division rings, frames, and an ingenious device allowing to force relations via terms in free modular lattices.

**Proposition 5.2.** For \( D \) as above and \( n \geq 3 \), \( \text{Th}_{eq}L(D^n) \) is undecidable.

**Proof.** The terms for an \( n \)-frame will either yield an \( n \)-frame of \( L(D^n) \) or just a single element. In the first case, one has terms giving elements of the ring associated with the frame or else a collapse of the frame. Again, considering relations on those ring elements one has terms enforcing these relations simultaneously - or else a collapse. Also, when applied to elements satisfying the relations, these remain unchanged. \( \square \)
6. Satisfiability problems

Dealing with modular lattices of finite height we consider 0 and 1 as constants.

**Lemma 6.1.** Let $L$ be an ML of height $n$ with an $n$-frame $a_{ij}$. For any pair $f(x), g(x)$ of lattice terms one can construct lattice polynomials $f^-(x), g^+(x)$ with constants $a_{ij}$ such that the following are equivalent

1. $L \models \exists x. f(x) < g(x)$
2. $L \models \exists x. f^-(x) = 0 \& g^+(x) = 1$

If $L$ admits an involution such that $a_{jj} \leq a_{ii}^j$ for $j \neq i$, then one can construct $h(x, y)$ and add

3. $L \models \exists x. h(x, y) = 1$

Construction and identification of the output polynomials, as well as reconstruction of the input terms can all be done in PTIME.

**Proof.** Define $b_k = \sum_{i \leq k} a_{ii}$, $f^-_k = a_{kk} (b_k - 1 + f)$, and $f^- = \prod_k f^-_k$. Similarly, for $g^+$. Put $h = g(x) \tilde{f}(y)$ where $\tilde{f}$ arises from $f^-$ by interchanging $+$ and $\cdot$ and replacing the constants by the corresponding elements of the dual $n$-frame canonically associated with the given $n$-frame. In the case of MOLs this gives rise to a ternary discriminator polynomial on $L [9]$. □

**Theorem 6.2.** Let $F$ be a field and $n \geq 3$.

(i) With each polynomial $p(x)$ over $F$ one can associate lattice terms $p^-(y)$ and $p^+(y)$ such that

\[ F \models \exists y. p(x) = 0 \iff L(F^n) \models \exists y. p^-(y) = 0 \& p^+(y) = 1 \]

(ii) With any pair $s(y), t(y)$ of lattice terms on can associate polynomials $p_1(x), \ldots, p_n(x)$ with integer coefficients such that

\[ L(F^n) \models \exists y. s(y) = 0 \& t(y) = 1 \iff F \models \exists x. p_1(x) = \ldots = p_n(x) = 0 \]

(iii) If $F^n$ admits an inner product $\Phi$ then with any ortholattice term $t(y)$ one can associate integer $p_i(x)$ such that

\[ L(F^n, \Phi) \models \exists y. t(y) = 1 \iff F \models \exists x. p_1(x) = \ldots = p_n(x) = 0 \]

All this can be done in PTIME and does not depend on $F$ for polynomials with integer coefficients.

Here, we conceive the $p(x)$ primarily as terms. But, as far as solvability is concerned, transition to a linear combination of monomials can be done in PTIME - adding variables.
Proof. In (i) use the lattice terms providing an \( n \)-frame and the interpretation of \( F \) into \( L(F^n) \). In (ii) and (iii) replace the (ortho)lattice variables by matrices with variables for elements of \( F \) and recall the descriptions of joins, meets, and orthocomplements in \( \mathcal{L}(F^{n \times n}) \). Solving \( t(\mathbf{f}) = 1 \) amounts to capturing the identity matrix. \( \square \)

**Corollary 6.3.** Let \( F \) be a subfield of \( \mathbb{R} \) and \( \Phi \) the canonical scalar product on \( F^n \) where \( n \geq 3 \). Then the following satisfiability problems are polynomially equivalent:

\[
\begin{align*}
L(F^n) & \models \exists \mathbf{f}. f(\mathbf{f}) < g(\mathbf{f}) & f \leq g \text{ lattice terms} \\
L(F^n) & \models \exists \mathbf{f}. f(\mathbf{f}) = 0 \& g(\mathbf{f}) = 1 & f, g \text{ lattice terms} \\
L(F^n, \Phi) & \models \exists \mathbf{t}. t(\mathbf{f}) = 1 & t \text{ ortholattice term} \\
F & \models \exists \mathbf{p}. p(\mathbf{f}) = 0 & p \text{ integer polynomial}
\end{align*}
\]

As remarked by George McNulty, decidability of the latter is an open and controversial question for \( F = \mathbb{Q} \) [20]. To get \( p \) from the \( p_i \) put \( p = \sum_i p_i^2 \).

7. **REAL COMPLEXITY**

Henceforth, we consider \( \mathbb{R}^n \) and \( \mathbb{C}^n \) always with the canonical scalar product \( \Phi \).

**Corollary 7.1.** The decision problems for each single \( \text{Th}_{eq}L(\mathbb{R}^n, \Phi) \), \( n \geq 3 \), as well as for \( \text{Th}_{eq}N \) are polynomially equivalent and \( \text{coBP}(NP^0_\mathbb{R}) \)-complete. In particular, they are \( \text{coNP-hard} \) and in \( \text{PSPACE} \).

Here, \( \text{BP}(NP^0_\mathbb{R}) \) refers to non-deterministic polynomial time in the Blum-Shub-Smale model of real computation with constants 0, 1, only, and binary input.

Proof. The equational theory of a class \( \mathcal{C} \) is just the complement of the set of sentences \( \exists \mathbf{f}. t(\mathbf{f}) = 1 \) satisfiable in some member of \( \mathcal{C} \). Thus, the claim about the \( L(\mathbb{R}^n, \Phi) \) follows from Cor.6.3 and the fact that feasibility of integer polynomials over \( \mathbb{R} \) is known to be \( \text{BP}(NP^0_\mathbb{R}) \)-complete cf. [17]. Also, with Prop.1 it follows that \( \text{Th}_{eq}N \) is in \( \text{coBP}(NP^0_\mathbb{R}) \). To prove completeness, we interpret feasibility of integer polynomials via 3-frames into \( L(\mathbb{R}^{3n}, \Phi) \) for all \( n \geq 1 \) simultaneously: according to \( L(\mathbb{R}^{3n}) \cong L((\mathbb{R}^n \times n)^3) \) we see the \( x_i \) as variables for matrices \( A_i \in \mathbb{R}^{n \times n} \). Imposing the relations \( A_i = A_i^t \) and \( A_i A_j = A_j A_i \), which we can enforce via ortholattice terms to be built into the identity \( t(\mathbf{t}) = 1 \), we achieve that the \( A_i \) are simultaneously diagonalizable, whence from \( p(\mathbf{A}) = 0 \) we obtain a solution in \( \mathbb{R} \). The cases \( 3n + 1 \) and \( 3n + 2 \) are dealt with considering the \( 3n \)-part of the frame. \( \square \)
8. MOL-representations

Given an inner product space \((V, \Phi)\) which is an elementary extension of an unitary space, an \(e\)-unitary representation of an MOL \(L\) is a \(0\)-lattice embedding \(\varepsilon : L \to L(V)\) such that

\[\varepsilon(a') = \varepsilon(a)^\perp \text{ for all } a \in L.\]

**Theorem 8.1.** Bruns, Roddy, H. [2, 8, 11]. For any \(e\)-unitary representation of an MOL, there is an atomic MOL \(\tilde{L}\) which is a sublattice of \(L(V)\) and contains both \(\varepsilon(L)\) and \(L(V, \Phi)\) as sub-OLs.

**Proposition 8.2.** H., Roddy [8, 11]. \(L \in \mathcal{N}\) if \(L\) admits an \(e\)-unitary representation. For subdirectly irreducibles, the converse holds, too.

**Proof.** Prop.1 and the fact, that all sections of fixed finite height have the same first order theory. Conversely, by the Jónsson Lemma we have \(L \in \text{HSP}_u\{L(C^n) \mid n < \infty\}\) and show that representability is preserved. \(\square\)

9. \(\ast\)-Regular Rings and Representations

An associative ring (with or without unit) \(R\) is (von Neumann) regular if for any \(a \in R\) there is a quasi-inverse \(x \in R\) such that \(axa = a\). A \(\ast\)-ring is a ring with an involution \(\ast\) as additional operation:

\[(x + y)^\ast = x^\ast + y^\ast, \quad (xy)^\ast = y^x x^\ast, \quad x^{**} = x.\]

\(e\) is a projection if \(e = e^\ast = e^2\). A \(\ast\)-ring is \(\ast\)-regular if it is regular and, moreover, positive: \(xx^\ast = 0\) only for \(x = 0\). Equivalently, for any \(a \in R\) there is a (unique) projection \(e\) such that \(aR = eR\). Examples are the \(\mathbb{C}^{n \times n}\) with \(r^\ast\) the adjoint matrix. The projections of a \(\ast\)-regular ring with unit form an MOL \(\overline{L}(R)\) where \(e \leq f \iff e = ef\) and \(e' = 1 - e\).

Now, \(e \mapsto eR\) is an isomorphism of \(\overline{L}(R)\) onto the ortholattice of principal right ideals of \(R\) and we may use the same notation for both.

Let \((V, \Phi)\) be an elementary extension of a unitary space. Denote by \(\phi^\ast\) the adjoint of \(\phi\) - if it exists. An \(e\)-unitary representation of a \(\ast\)-ring \(R\) is a ring embedding \(\iota : R \to \text{End}(V)\) such that \(\iota(r^\ast) = \iota(r)^\ast\) for any \(r \in R\).

**Proposition 9.1.** Giudici [5]. If \(\iota : R \to \text{End}(V)\) is an \(e\)-unitary representation of the \(\ast\)-regular ring \(R\), then

\[\varepsilon(eR) = \text{Im} \iota(e)\]

is an \(e\)-unitary representation of the MOL \(\overline{L}(R)\) in \((V, \Phi)\).
10. VON NEUMANN ALGEBRAS

A von-Neumann algebra $M$ is an unital involutive $\mathbb{C}$-subalgebra of the algebra $B(H)$ of all bounded operators of a separable Hilbert space $H$ with $M = M''$ where $A' = \{ \phi \in B(H) \mid \phi \psi = \psi \phi \ \forall \phi \in A \}$ is the commutant of $A$. $M$ is finite if $rr^* = 1$ implies $r^*r = 1$. For such, the projections of $M$ form a (continuous) MOL $L(M)$. A finite von-Neumann algebra is a factor if its center is $\mathbb{C} \cdot 1$. Particular examples of finite factors are the algebras $\mathbb{C}^{n \times n}$ of all complex $n$-by-$n$-matrices.

**Theorem 10.1.** Murray-von-Neumann [18]. Any finite von-Neumann algebra factor is either isomorphic to $\mathbb{C}^{n \times n}$ for some $n < \infty$ (type I$_n$) or contains for any $n < \infty$ a subalgebra isomorphic to $\mathbb{C}^{n \times n}$ (type II$_1$).

**Theorem 10.2.** Murray-von-Neumann [18]. For every finite factor $M$, there is a $\ast$-regular ring $U(M)$ of unbounded operators on $H$ having $M$ as $\ast$-subring and such that $\phi^*$ is adjoint to $\phi$. Moreover, $M$ and $U(M)$ have the same projections.

**Theorem 10.3.** $U(M)$ admits an $\epsilon$-unitary representation.

*Proof.* By the Compactness Theorem, it suffices to consider countable $\ast$-subrings $R$ of $U(M)$. A representation of $R$ is constructed from the given Hilbert space $H$. Let $H_0$ be the intersection of all domains of operators $\phi \in R$. Define, recursively, $H_{n+1}$ as the intersection of $H_n$ and all preimages $\phi^{-1}(H_n)$ where $\phi \in R$. $H_\omega = \bigcap_{n<\omega} H_n$. Due to Murray and von Neumann, all $H_n$ and $H_\omega$ are dense in $H$. It easily follows, that $\varepsilon(\phi) = \phi|H_\omega$ defines a representation. □

**Corollary 10.4.** $\text{Th}_{\text{eq}} \mathbb{N} = \text{Th}_{\text{eq}} L(M)$ for any finite von Neumann algebra factor $M$ of infinite dimension.

*Proof.* Observe $L(M) \cong \overline{L(U(M))}$ and apply Prop.8.2 and 9.1. □

**Corollary 10.5.** For any finite von Neumann algebra factors $M$ and $N$

$$U(N) \in \text{HSP}_u U(M), \ U(N) \in \text{HSP}_u \{ \mathbb{C}^{n \times n} \mid n < \infty \}$$

and, analogously, for the projection lattices.

*Proof.* With suitable choice of quasi-inverse, $\ast$-regular rings form a congruence distributive variety - the congruence lattice of $R$ is isomorphic to that of $\overline{L(R)}$. The $L(M)$ are simple. Thus, the Jónsson Lemma can be applied. □

A question, raised by Connes and still unanswered, asks whether the Banach-space version of this result is true.
References

[22] A. Tarski, A Decision Method for Elementary Algebra and Geometry, RAND Corporation, Santa Monica, Calif. 1948