The Complexity of Satisfiability Problems over Finite Lattices

Bernhard Schwarz

Department of Computer Science, University of Würzburg
schwarzb@informatik.uni-wuerzburg.de

Abstract. We study the computational complexity of problems defined by formulas over fixed finite lattices. We consider evaluation, satisfiability, tautology, counting, and quantified formulas. It turns out that evaluation and tautology always can be decided in alternating logarithmic time. For satisfiability we obtain the following dichotomy result: If the lattice is distributive, satisfiability is in alternating logarithmic time. Otherwise, it is NP-complete. Counting is #P-complete for every lattice with at least two elements. For quantified formulas over non-distributive lattices we obtain PSPACE-completeness, while the problem is in alternating logarithmic time, if the lattice is distributive.

1 Introduction

Goldmann and Russell [GR99] investigated the computational complexity of determining if an equation over some fixed finite group has a solution. Formally, an equation over a group $\mathcal{G} = (G, \circ)$ or more generally over an algebra $\mathcal{A} = (A, f_1, \ldots, f_m)$, is given as

$$H(x_1, \ldots, x_n) = a$$

where H is a formula over the variables $x_1, \ldots, x_n$, the constants $c \in A$, and the functions $f_1, \ldots, f_m$, and $a \in A$ is the target. The satisfiability problem over $\mathcal{A}$ (which we will denote $\mathrm{SAT}_{\mathcal{A}}$) is to determine if there is an assignment to the variables such that the equation is satisfied. Goldmann and Russell [GR99] showed, that this problem lies in P for nilpotent groups, but is NP-complete for any non-solvable group. Barrington et al. [BMMTT00] extended these results by considering the computational complexity of satisfiability over a fixed finite monoid.

Satisfiability over the boolean algebra $\mathcal{B} = (\{0,1\}, \{\wedge, \vee, \neg\})$, is the classical NP-complete problem [Co71], while satisfiability over the monotone boolean algebra $\mathcal{M} = (\{0,1\}, \{\wedge, \vee\})$, considering only monotone boolean formulas, can be decided in alternating logarithmic time.

Formulas over lattices generalize monotone formulas. A lattice is a partially ordered set with the functions $\wedge$ (greatest lower bound) and $\vee$ (smallest upper bound). While the monotone boolean algebra $\mathcal{M}$ is a distributive lattice, lattices in general can be non-distributive. We study the computational complexity of problems defined by formulas over both, distributive and non-distributive finite lattices. We observe the following dichotomy for a finite lattice V:

$$\begin{aligned} V \text{ is distributive} \quad &\Rightarrow \quad \text{Satisfiability over } V \text{ is in ALOGTIME.} \\ V \text{ is non-distributive} \quad &\Rightarrow \quad \text{Satisfiability over } V \text{ is NP-complete.} \end{aligned}$$

The paper is organized as follows. In Section 2 we define the problems to study over arbitrary algebras. We recall results that lead to monotone formulas and finally to finite lattices. Section 3 introduces lattices and classifies the tautology and counting problems for lattices. Section 4 deals with distributive lattices. We show that most problems are easy in this case. In Section 5 we complete the dichotomy, proving several completeness results for non-distributive lattices. The last section gives an overview of all results, and mentions open problems.

We use standard notations [Bu87,Pa94,GJ79]. Proofs that are given in sketch due to space constraints are presented in full in the appendix.

2 Algebras

We study problems that are defined by formulas over algebras. An *algebra* is a pair of sets (A, M) where A is a set of elements and $M \subseteq \{f : A^{n_f} \to A\}$ is a set of total functions. The algebra is called *finite*, if A and M are finite.

Definition 1. *For an algebra $\mathcal{A} = (A, M)$ the set of all $\mathcal{A}$-*formulas $\mathrm{F}(\mathcal{A})$ *is given by*

(1) *For each $a \in A : a$ is an $\mathcal{A}$-formula (constant).*
(2) *For each $i \geq 1 : x_i$ is an $\mathcal{A}$-formula (variable).*
(3) *If $F_1, \ldots, F_n$ are $\mathcal{A}$-formulas, and $f \in M$ is a function $f : A^n \to A$, then $f(F_1, \ldots, F_n)$ is an $\mathcal{A}$-formula.*

For an $\mathcal{A}$-formula $F \in \mathrm{F}(\mathcal{A})$, n_F denotes the number of different indices of variables occuring in F. Let $i_1 < \ldots < i_{n_F}$ be all indices of variables in F. For arbitrary $w = (a_1, \ldots, a_{n_F}) \in A^{n_F}$, $F(w)$ denotes the *value* of F, when replacing each x_{i_j} by a_j and applying the functions occuring in F. We also write $F(x_1, \ldots, x_n)$ to make clear that F is an $\mathcal{A}$-formula that contains at most the variables $x_1, \ldots, x_n$.

Definition 2. *For a fixed algebra $\mathcal{A} = (A, M)$ and $a \in A$ we define the following problems:*

1. Evaluation problems

$$\begin{aligned}\mathrm{VAL}^a_{\mathcal{A}} &=_{\mathrm{df}} \{(F, w) \mid F \in \mathrm{F}(\mathcal{A}), w \in A^{n_F}, F(w) = a\}.\\ \mathrm{VAL}_{\mathcal{A}} &=_{\mathrm{df}} \{(F, w, b) \mid (F, w) \in \mathrm{VAL}^b_{\mathcal{A}}\}.\end{aligned}$$

2. Tautology problems

$$\begin{aligned}\mathrm{TAUT}^a_{\mathcal{A}} &=_{\mathrm{df}} \{F \in \mathrm{F}(\mathcal{A}) \mid \forall w \in A^{n_F} : F(w) = a\}.\\ \mathrm{TAUT}_{\mathcal{A}} &=_{\mathrm{df}} \{(F, b) \mid F \in \mathrm{TAUT}^b_{\mathcal{A}}\}.\end{aligned}$$

3. Satisfiability problems

$$\begin{aligned}\mathrm{SAT}^a_{\mathcal{A}} &=_{\mathrm{df}} \{F \in \mathrm{F}(\mathcal{A}) \mid \exists w \in A^{n_F} : F(w) = a\}.\\ \mathrm{SAT}_{\mathcal{A}} &=_{\mathrm{df}} \{(F, b) \mid F \in \mathrm{SAT}^b_{\mathcal{A}}\}.\end{aligned}$$

4. Counting problems

$$\begin{aligned}\#^a_{\mathcal{A}}(F) &=_{\mathrm{df}} \#\{w \in A^{n_F} \mid F(w) = a\}\\ \#_{\mathcal{A}}(F, b) &=_{\mathrm{df}} \#^b_{\mathcal{A}}(F)\end{aligned}$$

5. Problems of quantified formulas
If we have a sequence of quantifiers $Q_1, \ldots, Q_n \in \{\forall, \exists\}$, then we define the number of alternations $\kappa(Q_1 \cdots Q_n) =_{\mathrm{df}} \#\{i \in \mathbb{N} \mid 1 \leq i \leq n-1, Q_i \neq Q_{i+1}\}$. *Now define for $k \geq 1$ the following:*

$$\begin{aligned}\mathrm{QAF}^a_{\mathcal{A}} &=_{\mathrm{df}} \{Q_1 \ldots Q_n F \mid F \in \mathrm{F}(\mathcal{A}), n = n_F, Q_1, \ldots, Q_n \in \{\forall, \exists\},\\ &\qquad Q_1 a_1 \in A \cdots Q_n a_n \in A : F(a_1, \ldots, a_n) = a\}.\\ \mathrm{QAF}_{\mathcal{A}} &=_{\mathrm{df}} \{(qF, b) \mid qF \in \mathrm{QAF}^b_{\mathcal{A}}\}.\\ \Sigma^a_{k,\mathcal{A}} &=_{\mathrm{df}} \{Q_1 \ldots Q_n F \in \mathrm{QAF}^a_{\mathcal{A}} \mid Q_1 = \exists, \kappa(Q_1 \cdots Q_n) = k-1\}.\\ \Sigma_{k,\mathcal{A}} &=_{\mathrm{df}} \{(qF, b) \mid qF \in \Sigma^b_{k,\mathcal{A}}\}.\\ \Pi^a_{k,\mathcal{A}} &=_{\mathrm{df}} \{Q_1 \ldots Q_n F \in \mathrm{QAF}^a_{\mathcal{A}} \mid Q_1 = \forall, \kappa(Q_1 \cdots Q_n) = k-1\}.\\ \Pi_{k,\mathcal{A}} &=_{\mathrm{df}} \{(qF, b) \mid qF \in \Pi^b_{k,\mathcal{A}}\}.\end{aligned}$$

These definition are a generalization of the well known problems.
If the algebra is finite, we can determine upper bounds for the problems:

Theorem 3. *Let $\mathcal{A} = (A, M)$ be a finite algebra, $a \in A$ and $k \geq 1$.*

1. $\mathrm{VAL}_{\mathcal{A}} \in \mathrm{ALOGTIME}$ *and* $\mathrm{VAL}^a_{\mathcal{A}} \in \mathrm{ALOGTIME}$.
2. $\mathrm{TAUT}_{\mathcal{A}} \in \mathrm{coNP}$ *and* $\mathrm{TAUT}^a_{\mathcal{A}} \in \mathrm{coNP}$.
3. $\mathrm{SAT}_{\mathcal{A}} \in \mathrm{NP}$ *and* $\mathrm{SAT}^a_{\mathcal{A}} \in \mathrm{NP}$.
4. $\#_{\mathcal{A}} \in \#\mathrm{P}$ *and* $\#^a_{\mathcal{A}} \in \#\mathrm{P}$.
5. $\Sigma_{k,\mathcal{A}} \in \Sigma^{\mathrm{P}}_k$, $\Pi_{k,\mathcal{A}} \in \Pi^{\mathrm{P}}_k$, $\mathrm{QAF}_{\mathcal{A}} \in \mathrm{PSPACE}$ *and* $\Sigma^a_{k,\mathcal{A}} \in \Sigma^{\mathrm{P}}_k$, $\Pi^a_{k,\mathcal{A}} \in \Pi^{\mathrm{P}}_k$, $\mathrm{QAF}^a_{\mathcal{A}} \in \mathrm{PSPACE}$.

Proof. The first statement follows from a result by Buss [Bu87]: Every parenthesis context-free language is in ALOGTIME. The other statements are trivial, since $\mathcal{A}$ is finite.

Theorem 3 cannot be improved in general, since the upper bounds are strict in the case of the boolean algebra:

Theorem 4. *Let be $\mathcal{B} =_{\mathrm{df}} (\{0,1\}, \{\wedge, \vee, \neg\})$ and $k \geq 1$.*

1. $\mathrm{VAL}^1_{\mathcal{B}}$ *is* $\leq^{logtime}_m$*-complete for* ALOGTIME.
2. $\mathrm{SAT}^1_{\mathcal{B}}$ *is* $\leq^{log}_m$*-complete for* NP.
3. $\mathrm{TAUT}^1_{\mathcal{B}}$ *is* $\leq^{log}_m$*-complete for* coNP.
4. $\#^1_{\mathcal{B}}$ *is* $\leq^{log}_m$*-complete for* $\#\mathrm{P}$.
5. $\Sigma^1_{k,\mathcal{B}}$, $\Pi^1_{k,\mathcal{B}}$, *and* $\mathrm{QAF}^1_{\mathcal{B}}$, *resp. are* $\leq^{log}_m$*-complete for* Σ^{P}_k, Π^{P}_k, *and* PSPACE, *resp.*

On the other hand, if we drop the negation, most problems turn to be easy:

Theorem 5. *Let be $\mathcal{M} =_{\mathrm{df}} (\{0,1\}, \{\wedge, \vee\})$.*

1. $\mathrm{VAL}^1_{\mathcal{M}} \in \mathrm{ALOGTIME}$.
2. $\mathrm{SAT}^1_{\mathcal{M}} \in \mathrm{ALOGTIME}$.
3. $\mathrm{TAUT}^1_{\mathcal{M}} \in \mathrm{ALOGTIME}$.
4. $\#^1_{\mathcal{M}}$ *is* $\leq^{log}_{1-T}$*-complete for* $\#\mathrm{P}$. *If* $\#^1_{\mathcal{M}}$ *is* $\leq^p_m$*-complete for* $\#\mathrm{P}$ *then* $\mathrm{P} = \mathrm{NP}$.
5. $\Sigma^1_{k,\mathcal{M}}, \Pi^1_{k,\mathcal{M}}, \mathrm{QAF}^1_{\mathcal{M}} \in \mathrm{ALOGTIME}$.

Turning to finite lattices, we show that non-distributivity nearly replaces the negation in the different results of Theorem 4 and Theorem 5.

3 Lattices

Now we want to study lattices. For binary functions it is usual to use infix notation. The previous results hold unchanged in this case. An algebra $V = (V, \{\wedge, \vee\})$ is called *lattice*, if both binary functions $\wedge$ and $\vee$ are commutative and associative, and if they satisfy

(1) $\forall a, b \in V : (a \wedge b) \vee b = b$ and
(2) $\forall a, b \in V : (a \vee b) \wedge b = b$.

In a lattice V we can define a *partial order* $\leq$ by $a \leq b \Leftrightarrow_{\mathrm{df}} a \wedge b = a$. So we have usual relations like $<$, $>$ and $\geq$.

Definition 6. *An element $a \in V$ is called* a direct predecessor *of $b \in V$, if*

(1) *$a < b$ and*
(2) $\{v \in V \mid a \leq v \leq b\} = \{a, b\}$.

We denote this as $a <_1 b$, and we call a and b neighbours.

Now we determine a lower bound for the counting problems in finite lattices:

Theorem 7. *If V is a finite lattice with at least two elements, then the counting problem $\#^v_V$ for any $v \in V$ is $\leq^{log}_{1-T}$-complete for $\#\mathrm{P}$.*

Proof (sketch). Let $a \in V$ be a direct predecessor of $b \in V$. We reduce #3SAT to $\#^a_V$ and $\#^b_V$. Define $f(x) =_{\mathrm{df}} ((x \vee a) \wedge b)$ and divide V into the sets $V_0 =_{\mathrm{df}} \{v \in V \mid f(v) = a\}$ and $V_1 =_{\mathrm{df}} \{v \in V \mid f(v) = b\}$. Let F be an instance of 3SAT with variables $x_1, \ldots, x_n$. Replace every literal x_k ($\neg x_k$, resp.) by $f(x_k)$ ($f(x_{k+n})$, resp.). We obtain a V-formula $H_0(x_1, \ldots, x_{2n})$. Let $H_1 =_{\mathrm{df}} \bigwedge_{i=1}^n (f(x_i) \vee f(x_{n+i}))$, $H_2 =_{\mathrm{df}} \bigvee_{i=1}^n (f(x_i) \wedge f(x_{n+i}))$, and $H_3 =_{\mathrm{df}} ((H_0 \wedge H_1) \vee H_2)$. We obtain:

$$\begin{aligned}
\#3\mathrm{SAT}(F) \cdot |V_0 \times V_1|^n &= \#^b_V(H_3) - \#^b_V(H_2) \\
&= \#^b_V(H_3) - (|V|^{2n} - (|V|^2 - |V_1|^2)^n) \\
&= (|V|^2 - |V_1|^2)^n - \#^a_V(H_3)
\end{aligned}$$

So #3SAT is $\leq^{log}_{1-T}$-reducible to $\#^a_V$ and $\#^b_V$.

Corollary 8. *If V is a finite lattice with at least two elements, then the counting problem $\#_V$ is $\leq^{log}_{1-T}$-complete for $\#\mathrm{P}$.*

In a finite lattice V we always have a *bottom element* $0 =_{\mathrm{df}} \bigwedge\limits_{v \in V} v$ and a *top element* $1 =_{\mathrm{df}} \bigvee\limits_{v \in V} v$. These elements satisfy $(\forall v \in V : 0 \leq v \leq 1)$.
Then the monotonity of the functions $\wedge$ and $\vee$ gives us the following Proposition:

Proposition 9. *Let V be a finite lattice, $H(x_1, \ldots, x_n) \in \mathrm{F}(V)$ and $a \in V$. Then the following equivalence holds:*

$$(\forall w \in V^n : H(w) = a) \Leftrightarrow H(0^n) = H(1^n) = a.$$

Theorem 10. *Let V be a finite lattice and let be $a \in V$. Then the problems TAUT_V and TAUT^a_V belong to* ALOGTIME.

Proof. Using Proposition 9 it is easy to reduce a tautology problem to an evaluation problem. So the tautology problems belong to ALOGTIME.

Theorem 11. *Let V be a finite lattice, $k \geq 1$, and $a \in V$. It holds:*

$$\Sigma^a_{2k,V}, \Sigma_{2k,V} \in \Sigma^{\mathrm{P}}_{2k-1}, \quad \textit{and} \quad \Pi^a_{2k+1,V}, \Pi_{2k+1,V} \in \Pi^{\mathrm{P}}_{2k}.$$

Proof. The last quantifier in a quantified formula of the given problems is $\forall$. So let $Q_1, \ldots, Q_n \in \{\forall, \exists\}$ and $i \in \mathbb{N}$ with $\exists = Q_i \neq Q_{i+1} = \ldots = Q_n = \forall$. It holds:

$$\begin{gathered}
Q_1 \cdots Q_n F(x_1, \ldots, x_n) \in \mathrm{QAF}^a_V \\
\text{if and only if} \\
Q_1 a_1 \in V \cdots Q_i a_i \in V : F(a_1, \ldots, a_i, x_{i+1}, \ldots, x_n) \in \mathrm{TAUT}^a_V.
\end{gathered}$$

After Theorem 10 we know $\mathrm{TAUT}^a_V \in \mathrm{ALOGTIME} \subseteq \mathrm{P}$. Furthermore there is one alternation less in $Q_1 \cdots Q_i$ than in $Q_1 \cdots Q_n$.

4 Distributive Lattices

Distributivity is usually a property of a whole lattice, but we would like to introduce distributive elements, too. An element a of a lattice V is called *distributive*, if

$$\forall b, c \in V : a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad \text{and}$$
$$\forall b, c \in V : a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

A lattice is called *distributive*, if each element is distributive.

Proposition 12. *Let V be a lattice, $H(x_1, \ldots, x_n) \in \mathrm{F}(V)$ and $w \in V^n$. Each distributive element $a \in V$ satisfies:*

$$H(a, \ldots, a) \leq a \vee H(w) \quad \textit{and} \quad H(a, \ldots, a) \geq a \wedge H(w).$$

Proof. We prove both via the structure of H:

(1) $H(x_1, \ldots, x_n) = v \in V$:

$$H(a, \ldots, a) = H(w) \leq a \vee H(w) \quad \text{and} \quad H(a, \ldots, a) = H(w) \geq a \wedge H(w).$$

(2) $H(x_1, \ldots, x_n) = x_i$:

$$H(a, \ldots, a) = a \leq a \vee H(w) \quad \text{and} \quad H(a, \ldots, a) = a \geq a \wedge H(w).$$

(3) $H(x_1, \ldots, x_n) = (F(x_1, \ldots, x_n) \wedge G(x_1, \ldots, x_n))$:

$$\begin{aligned} H(a, \ldots, a) &= F(a, \ldots, a) \wedge G(a, \ldots, a) \\ &\leq (a \vee F(w)) \wedge (a \vee G(w)) \\ &= a \vee (F(w) \wedge G(w)) = a \vee H(w), \end{aligned}$$

and

$$\begin{aligned} H(a, \ldots, a) &= F(a, \ldots, a) \wedge G(a, \ldots, a) \\ &\geq (a \wedge F(w)) \wedge (a \wedge G(w)) \\ &= a \wedge (F(w) \wedge G(w)) = a \wedge H(w). \end{aligned}$$

(4) $H(x_1, \ldots, x_n) = (F(x_1, \ldots, x_n) \vee G(x_1, \ldots, x_n))$: Similar to (3).

Theorem 13. *Let V be a lattice, $H(x_1, \ldots, x_n) \in \mathrm{F}(V)$, and let $a \in V$ be a distributive element. Then the following equivalence holds:*

$$(\exists w \in V^n : H(w) = a) \Leftrightarrow H(a, \ldots, a) = a.$$

Proof. Let $H(x_1, \ldots, x_n) \in \mathrm{F}(V)$ and $w \in V^n$ such that $H(w) = a$. From Proposition 12 we obtain $a = (a \wedge H(w)) \leq H(a, \ldots, a) \leq (a \vee H(w)) = a$. So this yields $H(a, \ldots, a) = a$.
The converse is easy, since $a, \ldots, a \in V^n$.

Theorem 14. *Let V be a finite lattice and let $a \in V$ be a distributive element. Then the satisfiability problem* SAT_V^a *belongs to* ALOGTIME.

Proof. Using Theorem 13 it is easy to reduce the satisfiability problem SAT_V^a to the evaluating problem VAL_V^a. So SAT_V^a belongs to ALOGTIME.

Corollary 15. *Let V be a finite, distributive lattice. Then the satisfiability problem* SAT_V *belongs to* ALOGTIME.

Corollary 16. *Let V be a finite lattice and let $a \in V$ be a distributive element. If $\#_V^a$ is $\leq_m^p$-complete for $\#\mathrm{P}$ then $\mathrm{P} = \mathrm{NP}$.*

Theorem 17. *Let V be a finite lattice, $k \geq 1$, and let $a \in V$ be a distributive element. The problems $\Sigma_{k,V}^a$, $\Pi_{k,V}^a$, and QAF_V^a belong to* ALOGTIME.

Proof (sketch). It is sufficient to show $\mathrm{QAF}_V^a \in \mathrm{ALOGTIME}$. For $v \in \{0,1\}$ (bottom and top element in V) define $\beta_v^a(\forall) =_{\mathrm{df}} v$ and $\beta_v^a(\exists) =_{\mathrm{df}} a$. We show the following.

$$Q_1 \cdots Q_n F(x_1, \ldots, x_n) \in \mathrm{QAF}_V^a$$
$$\text{if and only if}$$
$$F(\beta_0^a(Q_1), \ldots, \beta_0^a(Q_n)) = F(\beta_1^a(Q_1), \ldots, \beta_1^a(Q_n)) = a.$$

For $n = 0$ this statement is obvious.
For $n \geq 0$: Let $F(x_1, \ldots, x_{n+1}) \in \mathrm{F}(V)$ be a V-formula and let $Q_1, \ldots, Q_{n+1} \in \{\forall, \exists\}$. We define $G(x,y) =_{\mathrm{df}} F(x, \beta_y^a(Q_2), \ldots, \beta_y^a(Q_{n+1}))$. By induction hypothesis, it remains to prove the following for $Q \in \{\forall, \exists\}$:

$$(Qv \in V : G(v,0) = G(v,1) = a) \Leftrightarrow G(\beta_0^a(Q), 0) = G(\beta_1^a(Q), 1) = a.$$

$Q = \exists$: We use Theorem 13, since a is a distributive element.
$Q = \forall$: We use Propostion 9 and obtain:

$$(\forall v \in V : G(v,0) = G(v,1) = a) \Leftrightarrow G(0,0) = G(1,0) = G(0,1) = G(1,1) = a.$$

The monotonity of $\wedge$ and $\vee$ yields anyway $G(0,0) \leq G(0,1) \leq G(1,1)$ and $G(0,0) \leq G(1,0) \leq G(1,1)$, and we obtain

$$(\forall v \in V : G(v,0) = G(v,1) = a) \Leftrightarrow G(0,0) = G(1,1) = a.$$

So it is sufficient to evaluate F at the following two positions: Replace every $\exists$-quantified variable by a, and replace every $\forall$-quantified variable by 0 (1, resp.) for the first (second, resp.) evaluation. The quantified formula is in QAF_V^a if and only if both evaluations of F return the value a.

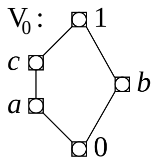
Now it is easy to reduce the problems $\Sigma_{k,V}^a$, $\Pi_{k,V}^a$, and QAF_V^a to an evaluation problem. So these problems belong to ALOGTIME.

Corollary 18. *Let V be a finite, distributive lattice and $k \geq 1$. Then the problems $\Sigma_{k,V}$, $\Pi_{k,V}$, and QAF_V belong to* ALOGTIME.

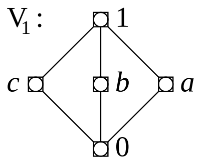
So most of the problems are easy in finite, distributive lattices. But what happens, if the finite lattice is non-distributive?

5 Non-distributive Lattices

According to Birkhoff [Bi67], each non-distributive lattice has at least one of the following two lattices as a sublattice:



Pentagon



Diamond

Definition 19. *Let V be a non-distributive lattice. A triple $(a,b,c) \in V^3$ such that*

(D1) $a \wedge b = c \wedge b$,
(D2) $a \vee b = c \vee b$, *and*
(D3) $a < c$ *or* ($a \neq c$, $a \wedge c = a \wedge b$ *and* $a \vee c = a \vee b$),

is called non-distributive.

Definition 20. *A non-distributive triple $(a,b,c) \in V^3$ is called* maximal non-distributive, *if each non-distributive triple $(a',b',c') \in V^3$ satisfies:*

(M1) $a' \wedge b' \not> a \wedge b$,
(M2) $a' \wedge b' = a \wedge b \Rightarrow a' \vee b' \not< a \vee b$,
(M3) $(a' \wedge b' = a \wedge b,\ a' \vee b' = a \vee b,\ a \not< c) \Rightarrow a' \not< c'$.

Obviously each finite non-distributive lattice has at least one such triple.

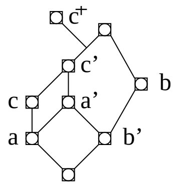
Lemma 21. *Let V be a lattice and let $(a,b,c) \in V^3$ be a maximal non-distributive triple. Then each $c^+ \in V$ satisfies:*

$$\left.\begin{array}{l}\text{(i) } c^+ \geq c \\ \text{(ii) } c^+ \not\geq c \vee b\end{array}\right\} \Rightarrow c^+ \wedge b = c \wedge b.$$

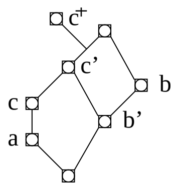
Proof (sketch). At first let us define a', b', $c' \in V$ by

(1) $b' =_{\text{df}} c^+ \wedge b$,
(2) $c' =_{\text{df}} b' \vee c$,
(3) $a' =_{\text{df}} b' \vee a$.

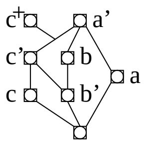
Supposing $b' = c^+ \wedge b \neq c \wedge b$ we get four cases, all of them leading to a contradiction:
Case 1: (C1) $a < c$. (Pentagon-case)
Case 1a: (C1a) $a' < c'$.
Here we obtain the following situation. (a', b, c') is a non-distributive triple, contradicting (M1):



Case 1b: (C1b) $a' = c'$.
Here we obtain the following situation. (a, b', c) is a non-distributive triple, contradicting (M2):



Case 2: $a \not< c$. (Diamond-case)
Case 2a: (C2a) $a' = a \vee b$.
Here we obtain the following situation. (b', a, b) is a non-distributive triple, contradicting (M3):



Case 2b: (C2b) $a' < a \vee b$.
Let $V' =_{\text{df}} \{v \in V \mid v \geq b'\}$. We get $a', b, c' \in V'$ and $(a' \vee c') \wedge b \gneq (a' \wedge b) \vee (c' \wedge b)$. This implies, that V' is a non-distributive sub-lattice. Hence V' contains at least one non-distributive triple, contradicting (M1).

So the assumption $b' = c^+ \wedge b \neq c \wedge b$ has lead to a contradiction to the maximallity of the non-distributive triple in every case.

Theorem 22. *Let V be a finite, non-distributive lattice. Then there exists a $c' \in V$, so that the satisfiability problem $\text{SAT}_V^{c'}$ is $\leq_m^{log}$-complete for* NP.

Proof. Let V be a finite, non-distributive lattice, $(a, b, c) \in V^3$ a maximal non-distributive triple, and $c' \in V$ such that $c \leq c' <_1 c \vee b$. We reduce 3SAT to $\text{SAT}_V^{c'}$.
Let F be an instance of 3SAT with variables $x_1, \ldots, x_n$:

$$F = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{3} x_{ij} \quad \text{with} \quad x_{ij} \in \{x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n\}.$$

First we define $f(x) =_{\text{df}} ((x \vee c') \wedge (c \vee b))$ and $n_{ij} =_{\text{df}} \begin{cases} k & \text{if } x_{ij} = x_k, \\ n + k & \text{if } x_{ij} = \neg x_k \end{cases}$

So we can define the following V-formulas:

$$\begin{aligned}
H_0(x_1, \ldots, x_{2n}) &=_{\text{df}} \bigwedge_{i=1}^{m} \bigvee_{j=1}^{3} f(x_{n_{ij}}), \\
H_1(x_1, \ldots, x_{2n}) &=_{\text{df}} \bigwedge_{i=1}^{n} (f(x_i) \vee f(x_{n+i})), \\
H_2(x_1, \ldots, x_{2n}) &=_{\text{df}} \bigvee_{i=1}^{n} (f(x_i) \wedge f(x_{n+i})), \\
H_0'(x_1, \ldots, x_{2n}) &=_{\text{df}} (H_0 \wedge b) \vee a, \\
H_1'(x_1, \ldots, x_{2n}) &=_{\text{df}} (H_1 \wedge b) \vee a, \\
H_2'(x_1, \ldots, x_{2n}) &=_{\text{df}} (H_2 \wedge b) \vee c', \quad \text{and} \\
H(x_1, \ldots, x_{2n}) &=_{\text{df}} H_0' \wedge H_1' \wedge H_2'.
\end{aligned}$$

With $c' <_1 c \vee b$ each $v \in V$ holds: $f(v) \in \{c', c \vee b\}$. So we get for each $w \in V^{2n}$: $H_0(w)$, $H_1(w)$, $H_2(w) \in \{c', c \vee b\}$. With $V_0 =_{\text{df}} \{v \in V \mid f(v) = c'\}$ and $V_1 =_{\text{df}} \{v \in V \mid f(v) = c \wedge b\}$ we can define Ω_y for each $y = (y_1, \ldots, y_n) \in \{0,1\}^n$:

$$\Omega_y =_{\text{df}} \{(w_1, \ldots, w_{2n}) \in V^{2n} \mid \forall i (1 \leq i \leq n) : (w_i, w_{n+i}) \in V_{y_i} \times V_{\overline{y_i}}\}.$$

We will show that

$$w \in \bigcup_{F(y)=1} \Omega_y \Leftrightarrow H(w) = c'.$$

First, let be $y \in \{0,1\}^n$ such that $F(y) = 1$, and let $w \in \Omega_y$. We can calculate $H_0(w) = c \vee b$, $H_1(w) = c \vee b$ and $H_2(w) = c'$. So we obtain $H_0'(w) = c \vee b$, $H_1'(w) = c \vee b$ and $H_2'(w) = c'$, and it holds $H(w) = c'$.
Now let $w = (w_1, \ldots, w_{2n}) \notin \bigcup_{F(y)=1} \Omega_I$. We obtain at least one of the following cases:

(1) $w \in \bigcup_{F(y)=0} \Omega_y$,
(2) $\exists i (1 \leq i \leq n) : f(w_i) = f(w_{n+i}) = c'$, or
(3) $\exists i (1 \leq i \leq n) : f(w_i) = f(w_{n+i}) = c \vee b$.

As consequences we obtain:

(1') $H_0(w) = c'$,
(2') $H_1(w) = c'$, or
(3') $H_2(w) = c \vee b$.

Using Lemma 21 we obtain

(1") $H'_0(w) = a$,
(2") $H'_1(w) = a$, or
(3") $H'_2(w) = c \vee b$.

If $H'_0(w) = a$ or $H'_1(w) = a$, then $H(w) \leq a$, so $H(w) \neq c'$, because $c' \not\leq a$. Otherwise $H'_0(w) = H'_1(w) = c \vee b$ and with (3") this yields $H(w) = c \vee b \neq c'$.
So each $w \notin \bigcup_{F(y)=1} \Omega_I$ satisfies $H(w) \neq c'$. Now we have:

$$F \in 3\mathrm{SAT} \Leftrightarrow H \in \mathrm{SAT}_V^{c'}.$$

The V-formula H is computable with input F by a log-space algorithm, so the satisfiability problem $\mathrm{SAT}_V^{c'}$ is $\leq_m^{log}$-complete for NP.

This completes the dichotomy to Corollary 15:

Theorem 23. *Let V be a finite lattice.*

$$\begin{aligned} V \textit{ is distributive} &\Rightarrow \mathrm{SAT}_V \in \mathrm{ALOGTIME}. \\ V \textit{ is non-distributive} &\Rightarrow \mathrm{SAT}_V \textit{ is } \leq_m^{log}\textit{-complete for } \mathrm{NP}. \end{aligned}$$

This is the main dichotomy result, and we will extend it by some completeness-results for quantified formulas over non-distributive lattices.

Let $\mathcal{B} =_{\mathrm{df}} (\{0,1\}, \{\wedge, \vee, \neg\})$. A $\mathcal{B}$-formula $F \in \mathrm{F}(\mathcal{B})$ is called *simple*, if $\neg$ only occurs at variables. Now we define the following problems:

$$\begin{aligned} \mathrm{SQBF} &=_{\mathrm{df}} \{Q_1 \cdots Q_n F(x_1, \ldots, x_n) \in \mathrm{QAF}^1_{\mathcal{B}} \mid F \text{ is simple}\}, \\ \Sigma_k\text{–SQBF} &=_{\mathrm{df}} \{Q_1 \cdots Q_n F(x_1, \ldots, x_n) \in \Sigma^1_{k,\mathcal{B}} \mid F \text{ is simple}\}, \\ \Pi_k\text{–SQBF} &=_{\mathrm{df}} \{Q_1 \cdots Q_n F(x_1, \ldots, x_n) \in \Pi^1_{k,\mathcal{B}} \mid F \text{ is simple}\}. \end{aligned}$$

The following Theorem is well known:

Theorem 24. *For $k \geq 1$ the problem Σ_k–SQBF is $\leq_m^{log}$-complete for Σ_k^{P}, Π_k–SQBF is $\leq_m^{log}$-complete for Π_k^{P}, and SQBF is $\leq_m^{log}$-complete for PSPACE,*

Theorem 25. *Let V be a finite, non-distributive lattice and $k \geq 1$. Then there is a $c' \in V$ such that:*

$\Sigma^{c'}_{2k-1,V}$ *is $\leq_m^{log}$-complete for $\Sigma^{\mathrm{P}}_{2k-1}$,*
$\Pi^{c'}_{2k,V}$ *is $\leq_m^{log}$-complete for Π^{P}_{2k}, and*
$\mathrm{QAF}^{c'}_V$ *is $\leq_m^{log}$-complete for* PSPACE.

Proof. The proof of Theorem 22 does not need the formula F to be in 3CNF. It is sufficient, that F is simple. We obtain the V-formula H_0 from a simple instance F by replacing each occurence of x_i by $f(x_i)$ and replacing $\neg x_i$ by $f(x_{n+i})$.

So let $Q_1 \cdots Q_n F(x_1, \ldots, x_n)$ be an instance of SQBF. We are now using the notations of the proof of Theorem 22, in particular the elements $c', c \vee b \in V$, the function f, and the V-formula

$H(x_1,\ldots,x_{2n})$. Furthermore we define additional quantifiers $Q_{n+i} =_{\text{df}} \exists$ for $i = 1,\ldots,n$ and a mapping $\alpha : V \to \{0,1\}$ by

$$\forall v \in V : \alpha(v) =_{\text{df}} \begin{cases} 0 & \text{if } f(v) = c', \\ 1 & \text{if } f(v) = c \vee b. \end{cases}$$

Finally we define $\alpha_k(v_1,\ldots,v_k) =_{\text{df}} (\alpha(v_1),\ldots,\alpha(v_k))$ as a shortcut.
We prove by induction on $i (0 \le i \le n)$:

$$\begin{gathered} y \in \{0,1\}^i, Q_{i+1}\cdots Q_n F(y, x_{i+1},\ldots,x_n) \in \text{SQBF} \\ \Rightarrow \forall v \in \alpha_i^{-1}(y) : Q_{i+1}\cdots Q_{2n} H(v, x_{i+1},\ldots,x_{2n}) \in \text{QAF}_V^{c'} \end{gathered}$$

and

$$\begin{gathered} v \in V^i, Q_{i+1}\cdots Q_{2n} H(v, x_{i+1},\ldots,x_{2n}) \in \text{QAF}_V^{c'} \\ \Rightarrow Q_{i+1}\cdots Q_n F(\alpha_i(v), x_{i+1},\ldots,x_n) \in \text{SQBF}. \end{gathered}$$

Case $i = n$: Already shown in the proof of Theorem 22.
Case $i \le n$: Let $Q_i = \forall$ ($Q_i = \exists$, resp.).
First let $y \in \{0,1\}^{i-1}$ and $Q_i \cdots Q_n F(y, x_i,\ldots,x_n) \in \text{SQBF}$. Then we have:

$$Q_i y_i \in \{0,1\} : Q_{i+1}\cdots Q_n F(y, y_i, x_{i+1},\ldots,x_n) \in \text{SQBF},$$

which results in:

$$\begin{gathered} Q_{i+1}\cdots Q_n F(y, 0, x_{i+1},\ldots,x_n) \in \text{SQBF} \\ \text{and (or, resp.)} \\ Q_{i+1}\cdots Q_n F(y, 1, x_{i+1},\ldots,x_n) \in \text{SQBF}. \end{gathered}$$

By induction hypothesis, we obtain for all $v \in \alpha_{i-1}^{-1}(y)$:

$$\begin{gathered} \forall v_i \in \alpha^{-1}(0) : Q_{i+1}\cdots Q_{2n} H(v, v_i, x_{i+1},\ldots,x_{2n}) \in \text{QAF}_V^{c'} \\ \text{and (or, resp.)} \\ \forall v_i \in \alpha^{-1}(1) : Q_{i+1}\cdots Q_{2n} H(v, v_i, x_{i+1},\ldots,x_{2n}) \in \text{QAF}_V^{c'}. \end{gathered}$$

Furthermore $V = \alpha^{-1}(0) \cup \alpha^{-1}(1)$. (in particular: $c' \in \alpha^{-1}(0) \neq \emptyset$ and $c \vee b \in \alpha^{-1}(1) \neq \emptyset$) Hence it holds:

$$\forall v \in \alpha_{i-1}^{-1}(y) : Q_i v_i \in V : Q_{i+1}\cdots Q_{2n} H(v, v_i, x_{i+1},\ldots,x_{2n}) \in \text{QAF}_V^{c'}.$$

So we have: $\forall v \in \alpha_{i-1}^{-1}(y) : Q_i \cdots Q_{2n} H(v, x_i,\ldots,x_{2n}) \in \text{QAF}_V^{c'}$. Hence the first statement is proved. To prove the second statement, let $v \in V^{i-1}$ and $Q_i \cdots Q_{2n} H(v, x_i,\ldots,x_{2n}) \in \text{QAF}_V^{c'}$. Then we have:

$$Q_i v_i \in V : Q_{i+1}\cdots Q_{2n} H(v, v_i, x_{i+1},\ldots,x_{2n}) \in \text{QAF}_V^{c'}.$$

By induction hypothesis we get:

$$Q_i v_i \in V : Q_{i+1}\cdots Q_n F(\alpha_i(v, v_i), x_{i+1},\ldots,x_n) \in \text{SQBF}.$$

Together with $\alpha(V) = \{0,1\}$ this yields: $Q_i \cdots Q_n F(\alpha_{i-1}(v), x_i,\ldots,x_n) \in \text{SQBF}$.
This completes the proof of the second statement.

In particular, the two statements for $i = 0$ result in:

$$Q_1 \cdots Q_n F(x_1,\ldots,x_n) \in \text{SQBF} \Leftrightarrow Q_1 \cdots Q_{2n} H(x_1,\ldots,x_{2n}) \in \text{QAF}_V^{c'}.$$

Therefore we can reduce SQBF to $\text{QAF}_V^{c'}$.

The reduction does not change the number of alternations between $\forall$ and $\exists$, if the last quantifier is an $\exists$-quantifier.

Corollary 26. *Let V be a finite, non-distributive lattice and $k \geq 1$. Then $\Sigma_{2k-1,V}$ and $\Sigma_{2k,V}$ are $\leq_m^{log}$-complete for $\Sigma_{2k-1}^{\mathrm{P}}$, $\Pi_{2k,V}$ and $\Pi_{2k+1,V}$ are $\leq_m^{log}$-complete for Π_{2k}^{P}, and QAF_V is $\leq_m^{log}$-complete for* PSPACE.

Proof. Theorem 11 and Theorem 25.

This Corollary completes the dichotomy to Corollary 18.

Theorem 27. *Let V_1 be the "diamond"-lattice. The counting problem $\#_{\mathrm{V}_1}^c$ is $\leq_m^{log}$-complete for* #P.

Proof (sketch). We reduce #3SAT to $\#_{\mathrm{V}_1}^c$:
Let F be an instance of 3SAT with variables $x_1, \ldots, x_n$. Replace every literal x_k by $(x_k \vee b)$ and replace every literal $\neg x_k$ by $(x_{n+k} \vee b)$. We obtain a V_1-formula $H_3(x_1, \ldots, x_{2n})$. Furthermore let $H_1 =_{\mathrm{df}} \bigvee_{i=1}^n (((x_i \wedge x_{n+i}) \vee c) \wedge a)$, $H_2 =_{\mathrm{df}} \bigvee_{i=1}^n (((x_i \wedge x_{n+i}) \vee b) \wedge a)$, $H_4 =_{\mathrm{df}} \bigwedge_{i=1}^n (((x_i \vee c) \wedge a) \vee b)$, $H_5 =_{\mathrm{df}} \bigwedge_{i=1}^n (((x_{n+i} \vee c) \wedge a) \vee b)$, and $H =_{\mathrm{df}} H_1 \vee H_2 \vee (H_3 \wedge H_4 \wedge H_5 \wedge c)$.
We obtain:

$$\#_{\mathrm{V}_1}^c(H) = \#3\mathrm{SAT}(F)$$

So there are finite lattices, whose counting problems are $\leq_m^{log}$-complete for #P.

6 Results and Open Questions

Let V be a finite lattice with at least two elements, and $k \geq 1$.

Problem	Complexity of the problem, if V is distributive	non-distributive
VAL_V	ALOGTIME	ALOGTIME
SAT_V	ALOGTIME	$\leq_m^{log}$-complete for NP
TAUT_V	ALOGTIME	ALOGTIME
$\Sigma_{2k-1,V}$	ALOGTIME	$\leq_m^{log}$-complete for $\Sigma_{2k-1}^{\mathrm{P}}$
$\Sigma_{2k,V}$	ALOGTIME	$\leq_m^{log}$-complete for $\Sigma_{2k-1}^{\mathrm{P}}$
$\Pi_{2k,V}$	ALOGTIME	$\leq_m^{log}$-complete for Π_{2k}^{P}
$\Pi_{2k+1,V}$	ALOGTIME	$\leq_m^{log}$-complete for Π_{2k}^{P}
QAF_V	ALOGTIME	$\leq_m^{log}$-complete for PSPACE
$\#_V$	$\leq_{1-T}^{log}$-complete for #P if P $\neq$ NP : not $\leq_m^p$-complete for #P	$\leq_{1-T}^{log}$-complete for #P

For the "diamond"-lattice V_1 the counting problem $\#_{\mathrm{V}_1}$ is $\leq_m^{log}$-complete for #P. So the question arises, which non-distributive lattices have counting problems that are $\leq_m^p$-complete for #P?

It was shown that P $\neq$ NP implies that distributive lattices do not have counting problems, being $\leq_m^p$-complete for #P. But maybe this claim can be showen independently.

We showed that for a distributive element $a \in V$ the element-specific problem SAT_V^a is in ALOGTIME. On the other hand we showed, that in every non-distributive lattice V there is at least one element $c' \in V$, so that $\mathrm{SAT}_V^{c'}$ is $\leq_m^{log}$-complete for NP. Of course this element is not distributive. But which computational complexity has the problem SAT_V^a for an arbitrary not distributive element a?

Acknowledgments

I have benefited greatly from discussions with Klaus Wagner, and I want to thank Christian Glasser for helpful discussions.

References

[Bi67] G. Birkhoff, *Lattice Theory*, Colloquium Publications Vol. XXV, American Mathematical Society, Providence, RI, 1967.

[BMMTT00] D. M. Barrington, P. McKenzie, C. Moore, P. Tesson, and D. Therien, *Equation Satisfiability and Program Satisfiability for Finite Monoids*, Proceedings of the 25th International Symposium on Mathematical Foundations of Computer Science, pages 172-181, 2000.

[Bu87] S. R. Buss, *The Boolean formula value problem is in* ALOGTIME, Proceedings of the 19$^{\text{th}}$ Symposium on Theory of Computing, pages 123-131, 1987.

[Co71] S. A. Cook, *The complexity of theorem-proving procedures*, Proceedings of the Third ACM Symposium on Theory of Computing, pages 151-158, 1971.

[GJ79] M. R. Garey, D. S. Johnson, *Computers and Intractability*, W. H. Freeman and Company, 1979.

[GR99] M. Goldmann, A. Russell, *The complexity of solving equations over finite groups*, Proceedings of the 14th Annual IEEE Conference on Computational Complexity, pages 80-86, 1999.

[Pa94] C. H. Papadimitriou, *Computational Complexity*, Addison-Wesley, Reading, MA, 1994.

[Ru81] W. L. Ruzzo, *On uniform circuit complexity*, Journal of Computer System Sciences, 22:265-383, 1981

Appendix

Theorem 7. *If V is a finite lattice with at least two elements, then the counting problem $\#_V^v$ for any $v \in V$ is $\leq_{1-T}^{log}$-complete for* #P.

Proof. Let $a \in V$ be a predecessor of $b \in V$. We reduce #3SAT to $\#_V^a$ and $\#_V^b$. Let F be an instance of 3SAT with variables $x_1, \ldots, x_n$:

$$F = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{3} x_{ij} \quad \text{with} \quad x_{ij} \in \{x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n\}.$$

Now we define:

$$n_{ij} =_{\mathrm{df}} \begin{cases} k & \text{if } x_{ij} = x_k, \\ n+k & \text{if } x_{ij} = \neg x_k \end{cases}$$

and $f(x) =_{\mathrm{df}} ((x \vee a) \wedge b)$.
With $f(V) = \{a, b\}$ the function f devides V into two subsets:

$$V_0 =_{\mathrm{df}} \{v \in V \mid f(v) = a\} \quad \text{and} \quad V_1 =_{\mathrm{df}} \{v \in V \mid f(v) = b\}.$$

The following V-formulas are formulas over a and b, after evaluating the function f, so the value will always be a or b:

$$\begin{aligned}
H_0(x_1, \ldots, x_{2n}) &=_{\mathrm{df}} \bigwedge_{i=1}^{m} \bigvee_{j=1}^{3} f(x_{n_{ij}}), \\
H_1(x_1, \ldots, x_{2n}) &=_{\mathrm{df}} \bigwedge_{i=1}^{n} (f(x_i) \vee f(x_{n+i})), \\
H_2(x_1, \ldots, x_{2n}) &=_{\mathrm{df}} \bigvee_{i=1}^{n} (f(x_i) \wedge f(x_{n+i})), \\
H_3(x_1, \ldots, x_{2n}) &=_{\mathrm{df}} ((H_0 \wedge H_1) \vee H_2).
\end{aligned}$$

For each $y = (y_1, \ldots, y_n) \in \{0,1\}^n$ we define

$$\Omega_y =_{\mathrm{df}} \{(w_1, \ldots, w_{2n}) \in V^{2n} \mid \forall_{i=1}^{n} (w_i, w_{n+i}) \in V_{y_i} \times V_{\overline{y_i}}\}.$$

Now we are looking at the following sets:

$$\begin{aligned}
\Omega_2 &=_{\mathrm{df}} \{w \in V^{2n} \mid H_2(w) = b\}, \\
\Omega_3 &=_{\mathrm{df}} \{w \in V^{2n} \mid H_3(w) = b\}, \\
\Omega &=_{\mathrm{df}} \Omega_3 \backslash \Omega_2.
\end{aligned}$$

We will show: $\Omega = \bigcup_{F(y)=1} \Omega_y$. This union is disjunct, and all Ω_y have the same size. So #3SAT(F) is easy to calculate, when you know the size of Ω.

So we take at first $w = (w_1, \ldots, w_{2n}) \in \Omega$:
With $w \notin \Omega_2$ we have $H_2(w) = a$. Taking into account $H_3 = ((H_0 \wedge H_1) \vee H_2)$ we get $H_0(w) = b$, $H_1(w) = b$ and $H_2(w) = a$. This leads us to:

(1) $\forall i (1 \leq i \leq m) \exists j (1 \leq j \leq 3) : [f(w_{n_{ij}}) = b]$
(2) $\forall i (1 \leq i \leq n) : [f(w_i) = b$ or $f(w_{n+i}) = b]$
(3) $\forall i (1 \leq i \leq n) : [f(w_i) = a$ or $f(w_{n+i}) = a]$

Putting together the statements (2) and (3), we know $f(w_i) = b$ and $f(w_{n+i}) = a$, or the other way around. So $y = (y_1, \ldots, y_n) \in \{0,1\}^n$ is well defined by

$$\forall i (1 \le i \le n) : y_i =_{\mathrm{df}} \begin{cases} 1 & \text{if } f(w_i) = b \text{ and } f(w_{n+i}) = a, \\ 0 & \text{if } f(w_i) = a \text{ and } f(w_{n+i}) = b. \end{cases}$$

The construction gives us $w \in \Omega_y$, and statement (1) tells us $F(y) = 1$.

Now we take $w \in \bigcup_{F(y)=1} \Omega_y$. Here it is simple to calculate $w \in \Omega$.

Finally, each Ω_y has the size: $|\Omega_y| = |V_0 \times V_1|^n$.
Hence we get:

$$|\Omega| = |\bigcup_{F(y)=1} \Omega_y| = \sum_{F(y)=1} |V_0 \times V_1|^n = \#3\mathrm{SAT}(F) \cdot |V_0 \times V_1|^n.$$

On the other hand Ω_2 is a subset of Ω_3 and we get:

$$|\Omega| = |\Omega_3| - |\Omega_2| = \#^b_V(H_3) - \#^b_V(H_2).$$

Furthermore each $w \in V^{2n}$ holds $H_2(w) \in \{a, b\}$ and $H_3(w) \in \{a, b\}$, so we get:

$$\begin{aligned} \#^b_V(H_2) &= |V|^{2n} - \#^a_V(H_2) \text{ and} \\ \#^b_V(H_3) &= |V|^{2n} - \#^a_V(H_3). \end{aligned}$$

And finally:

$$\begin{aligned} \#3\mathrm{SAT}(F) \cdot |V_0 \times V_1|^n &= \#^b_V(H_3) - \#^b_V(H_2) \\ &= \#^b_V(H_3) - (|V|^{2n} - (|V|^2 - |V_1|^2)^n) \\ &= \#^a_V(H_2) - \#^a_V(H_3) \\ &= (|V|^2 - |V_1|^2)^n - \#^a_V(H_3). \end{aligned}$$

So $\#3\mathrm{SAT}$ is $\le^{log}_{1-T}$-reducible to $\#^a_V$ and $\#^b_V$.

Each element of a finite lattice with at least two elements has at least one neighbour, so the proof is done.

Theorem 17. *Let V be a finite lattice, $k \ge 1$, and let $a \in V$ be a distributive element. Then the problems $\Sigma^a_{k,V}$, $\Pi^a_{k,V}$ and QAF^a_V belong to* ALOGTIME.

Proof. It is sufficient to show $\mathrm{QAF}^a_V \in \mathrm{ALOGTIME}$. Therefore, we show that a quantified V-formula $Q_1 \cdots Q_n F(x_1, \ldots, x_n)$ is in QAF^a_V if and only if $F(w) = a$ for two fixed $w \in V^n$.

For $v \in \{0,1\}$ (bottom and top element in V) define $\beta^a_v(\forall) =_{\mathrm{df}} v$ and $\beta^a_v(\exists) =_{\mathrm{df}} a$. We show now by induction on $n \in \mathbb{N}$:

$$Q_1 \cdots Q_n F(x_1, \ldots, x_n) \in \mathrm{QAF}^a_V$$
$$\text{if and only if}$$
$$F(\beta^a_0(Q_1), \ldots, \beta^a_0(Q_n)) = F(\beta^a_1(Q_1), \ldots, \beta^a_1(Q_n)) = a.$$

For $n = 0$ this statement is obvious.
For $n \ge 0$ let $F(x_1, \ldots, x_{n+1}) \in \mathrm{F}(V)$ be a V-formula and let $Q_1, \ldots, Q_{n+1} \in \{\forall, \exists\}$ be some quantifiers.

$$G(x, y) =_{\mathrm{df}} F(x, \beta^a_y(Q_2), \ldots, \beta^a_y(Q_{n+1})).$$

By definition of QAF_V^a,

$$Q_1 \cdots Q_{n+1} F(x_1, \ldots, x_{n+1}) \in \mathrm{QAF}_V^a$$
$$\text{if and only if}$$
$$Q_1 a_1 \in V : Q_2 \cdots Q_{n+1} F(a_1, x_2, \ldots, x_{n+1}) \in \mathrm{QAF}_V^a.$$

By induction hypothesis, the latter is equivalent to

$$Q_1 a_1 \in V : G(a_1, 0) = G(a_1, 1) = a.$$

Hence it remains to prove for $Q \in \{\forall, \exists\}$ the following:

$$(Qv \in V : G(v, 0) = G(v, 1) = a) \Leftrightarrow G(\beta_0^a(Q), 0) = G(\beta_1^a(Q), 1) = a.$$

$\underline{Q = \exists}$: We can use Theorem 13, because a is a distributive element, to obtain:

$$(\exists v \in V : G(v, 0) = G(v, 1) = a) \Leftrightarrow G(a, 0) = G(a, 1) = a.$$

So the statement is proved for $Q = \exists$.

$\underline{Q = \forall}$: Here we can use Proposition 9, to obtain:

$$(\forall v \in V : G(v, 0) = a) \Leftrightarrow G(0, 0) = G(1, 0) = a \quad \text{and}$$
$$(\forall v \in V : G(v, 1) = a) \Leftrightarrow G(0, 1) = G(1, 1) = a.$$

The monotonity of $\wedge$ and $\vee$ gives us:

$$G(0, 0) \leq G(0, 1) \leq G(1, 1) \quad \text{and} \quad G(0, 0) \leq G(1, 0) \leq G(1, 1).$$

Hence we obtain

$$(\forall v \in V : G(v, 0) = G(v, 1) = a) \Leftrightarrow G(0, 0) = G(1, 1) = a.$$

So the statement is proved for $Q = \forall$, too.

So it is sufficient to evaluate F at the following two positions: Replace every $\exists$-quantified variable by a, and replace every $\forall$-quantified variable by 0 (1, resp.) for the first (second, resp.) evaluation. The quantified formula is in QAF_V^a if and only if both evaluations of F return the value a.

Now it is easy to reduce the problems $\Sigma_{k,V}^a$, $\Pi_{k,V}^a$ and QAF_V^a to an evaluation problem. So these problems belong to ALOGTIME.

Lemma 21. *Let V be a lattice, and let $(a, b, c) \in V^3$ be a maximal non-distributive triple. Then each $c^+ \in V$ satisfies:*

$$\left.\begin{array}{l}\text{(i) } c^+ \geq c \\ \text{(ii) } c^+ \not\geq c \vee b\end{array}\right\} \Rightarrow c^+ \wedge b = c \wedge b.$$

Proof. At first let us define a', b', $c' \in V$ by

(1) $b' =_{\mathrm{df}} c^+ \wedge b$,
(2) $c' =_{\mathrm{df}} b' \vee c$,
(3) $a' =_{\mathrm{df}} b' \vee a$.

Some direct consequences of these definitions are:

(1a) $b' \leq c^+$,

(1b) $b' \leq b$,
(2a) $c' \geq b'$,
(2b) $c' \geq c$,
(3a) $a' \geq b'$,
(3b) $a' \geq a$.

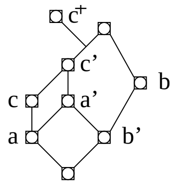
Furthermore it holds:

(4) $a \wedge b \overset{(D1)}{=} c \wedge b \overset{(i)}{\leq} c^+ \wedge b \overset{(1)}{=} b'$, which means $a \wedge b = c \wedge b \leq b'$,
(5) $c' \overset{(2)}{=} c \vee b' \overset{(1a)}{\leq} c \vee c^+ \overset{(i)}{=} c^+$, which means $c' \leq c^+$.

Suppose: $b' \neq c \wedge b$.
Using (4) we obtain $b' > c \wedge b$.
Case 1: (C1) $a < c$. (Pentagon-case)
It holds:

$$a' \overset{(3)}{=} b' \vee a \overset{(C1)}{\leq} b' \vee c \overset{(2)}{=} c', \text{ so we get } a' \leq c'.$$

Case 1a: (C1a) $a' < c'$.
We prove the following situation ((a', b, c') contradicting (M1)):



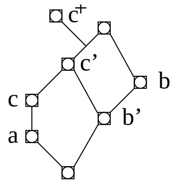
It holds:

(I) $b' \overset{(1b,3a)}{\leq} a' \wedge b \overset{(C1a)}{\leq} c' \wedge b \overset{(5)}{\leq} c^+ \wedge b \overset{(1)}{=} b'$,
(II) $a \vee b \overset{(3b)}{\leq} a' \vee b \overset{(C1a)}{\leq} c' \vee b \overset{(2)}{=} (c \vee b') \vee b \overset{(1b)}{\leq} c \vee b \overset{(D2)}{=} a \vee b$,

each with equality, so we have:

$$a' \wedge b \overset{(I)}{=} c' \wedge b,$$
$$a' \vee b \overset{(II)}{=} c' \vee b \text{ and}$$
$$a' \overset{(C1a)}{<} c'.$$

This means, (a', b, c') is a non-distributive triple with $a' \wedge b \overset{(I)}{=} b' > a \wedge b$, contradicting (M1).
Case 1b: (C1b) $a' = c'$.
Here we prove the following situation ((a, b', c) contradicting (M2)):



It holds:

(I) $a \wedge b \overset{(4)}{\leq} a \wedge b' \overset{(C1)}{\leq} c \wedge b' \overset{(1b)}{\leq} c \wedge b \overset{(D1)}{=} a \wedge b$ with equality, and
(II) $a \vee b' \overset{(3)}{=} a' \overset{(C1b)}{=} c' \overset{(2)}{=} c \vee b' \overset{(1b)}{\leq} c \vee b$.

We obtain $c' \leq c \vee b$ from (II). If $c' = c \vee b$, we obtain $c^+ \overset{(5)}{\geq} c' = c \vee b$, contradicting (ii). So we have $c' < c \vee b$. Furthermore we have:

$$a \wedge b' \overset{(\mathrm{I})}{=} c \wedge b',$$
$$a \vee b' \overset{(\mathrm{II})}{=} c \vee b' \text{ and}$$
$$a \overset{(\mathrm{C1})}{<} c.$$

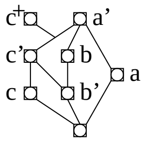
So (a, b', c) is a non-distributive triple with

$$a \wedge b' \overset{(\mathrm{I})}{=} a \wedge b \quad \text{and} \quad a \vee b' \overset{(\mathrm{II})}{=} c' < c \vee b \overset{(\mathrm{D2})}{=} a \vee b,$$

contradicting (M2).
This means case 1 cannot occur.
Case 2: $a \not< c$. (Diamond-case)
With (D3) we have:

(C2) $a \neq c$, $a \wedge c = a \wedge b$ and $a \vee c = a \vee b$,

and it holds: $a' \overset{(3)}{=} a \vee b' \overset{(1\mathrm{b})}{\leq} a \vee b$, so we obtain $a' \leq a \vee b$.
Case 2a: (C2a) $a' = a \vee b$.
Here we prove the following situation ((b', a, b) contradicting (M3)):



It holds:

(I) $a \wedge b \overset{(4)}{\leq} a \wedge b' \overset{(1\mathrm{b})}{\leq} a \wedge b$, with equality, and
(II) $a \vee b' \overset{(3)}{=} a' \overset{(\mathrm{C2a})}{=} a \vee b$.

Therefore,

$$b' \wedge a \overset{(\mathrm{I})}{=} b \wedge a,$$
$$b' \vee a \overset{(\mathrm{II})}{=} b \vee a \text{ and}$$
$$b' < b.$$

The last one ($b' < b$) follows by (1b), and because $b' = b$ would lead to

$$c^+ \overset{(5,1\mathrm{a})}{\geq} c' \vee b' \overset{(2\mathrm{b})}{\geq} c \vee b' = c \vee b \text{ (contradicting (ii))}.$$

So (b', a, b) is a non-distributive triple with

$$b' \wedge a = a \wedge b,\ b' \vee a = a \vee b \text{ and } b' < b, \text{ but } a \not< c,$$

contradicting (M3).
Case 2b: (C2b) $a' < a \vee b$.
Let $V' =_{\mathrm{df}} \{v \in V \mid v \geq b'\}$. We prove that V' contains a non-distributive triple, contradicting (M1). V' is a sub-lattice of V with $a', b, c' \in V'$. (3a,1b,2a)
Furthermore we have:

(I) $b' \overset{(2\mathrm{a},1\mathrm{b})}{\leq} c' \wedge b \overset{(5)}{\leq} c^+ \wedge b \overset{(1)}{=} b'$, with equality, and
(II) $b' \overset{(3\mathrm{a},1\mathrm{b})}{\leq} a' \wedge b \leq b$.

With (C2b) we obtain $a' \not\geq a \vee b$ and (3b) leads us to $a' \not\geq b$. So $a' \wedge b \neq b$ and with (II) we obtain $a' \wedge b < b$. Now it holds:

$$\begin{aligned}(a' \vee c') \wedge b &\overset{(3b,2b)}{\geq} (a \vee c) \wedge b \overset{(C2)}{=} (a \vee b) \wedge b = b\\ (a' \wedge b) \vee (c' \wedge b) &\overset{(I)}{=} (a' \wedge b) \vee b' \overset{(II)}{=} a' \wedge b < b\end{aligned}$$

So V' is a non-distributive sub-lattice of V, containing a non-distributive triple (a'', b'', c'') with $a'' \wedge b'' \geq b' > a \wedge b$, contradicting (M1).

Hence the assumption $b' = c^+ \wedge b \neq c \wedge b$ has lead to a contradiction to the maximallity of the non-distributive triple in every case.

Proposition 28. *Let* V_1 *be the "diamond"-lattice. Each* $v \in \mathrm{V}_1$ *holds:*

(1) $((v \vee c) \wedge a) \vee b = 1 \;\Leftrightarrow\; v \in \{a, b, 1\}$,

(2) $(v \vee c) \wedge a = 0 \;\Leftrightarrow\; v \in \{0, c\}$,

(3) $(v \vee b) \wedge a = 0 \;\Leftrightarrow\; v \in \{0, b\}$.

Theorem 27. *Let* V_1 *be the "diamond"-lattice. The counting problem* $\#^{c}_{\mathrm{V}_1}$ *is* $\leq^{log}_{m}$*-complete for* #P.

Proof. We reduce #3SAT to $\#^{c}_{\mathrm{V}_1}$:
Let F be an instance of 3SAT with variables $x_1, \ldots, x_n$:

$$F = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{3} x_{ij} \quad \text{with} \quad x_{ij} \in \{x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n\}.$$

Now we define

$$n_{ij} =_{\mathrm{df}} \begin{cases} k & \text{if } x_{ij} = x_k, \\ n + k & \text{if } x_{ij} = \neg x_k \end{cases}$$

and the V_1-formulas

$$\begin{aligned}
H_1 &=_{\mathrm{df}} \bigvee_{i=1}^{n} (((x_i \wedge x_{n+i}) \vee c) \wedge a),\\
H_2 &=_{\mathrm{df}} \bigvee_{i=1}^{n} (((x_i \wedge x_{n+i}) \vee b) \wedge a),\\
H_3 &=_{\mathrm{df}} \bigwedge_{i=1}^{m} (\bigvee_{j=1}^{3} x_{n_{ij}} \vee b),\\
H_4 &=_{\mathrm{df}} \bigwedge_{i=1}^{n} (((x_i \vee c) \wedge a) \vee b),\\
H_5 &=_{\mathrm{df}} \bigwedge_{i=1}^{n} (((x_{n+i} \vee c) \wedge a) \vee b),\\
H &=_{\mathrm{df}} H_1 \vee H_2 \vee (H_3 \wedge H_4 \wedge H_5 \wedge c).
\end{aligned}$$

These definitions give us for each $w \in \mathrm{V}_1^{2n}$:
$H_1(w) \leq a$, $H_2(w) \leq a$, $H_3(w) \geq b$, $H_4(w) \geq b$ and $H_5(w) \geq b$.

Finally for each $y = (y_1, \ldots, y_n) \in \{0,1\}^n$ we define $w_y = (w_1, \ldots, w_{2n}) \in \mathrm{V}_1^{2n}$ by

$$\forall i (1 \leq i \leq n) : (w_i, w_{n+i}) =_{\mathrm{df}} \begin{cases} (a, b) & \text{if } y_i = 1, \\ (b, a) & \text{if } y_i = 0. \end{cases}$$

We will show: $\{w \in \mathrm{V}_1^{2n} \mid H(w) = c\} = \{w_y \mid F(y) = 1\}$.
With all w_y being different, we then have $\#_{\mathrm{V}_1}^{c}(H) = \#3\mathrm{SAT}(F)$.

So we first take $w = (w_1, \ldots, w_{2n}) \in \mathrm{V}_1^{2n}$ with $H(w) = c$.
It holds:

$H_1(w) \leq c$, and with $H_1(w) \leq a$ we get $H_1(w) = 0$.
$H_2(w) \leq c$, and with $H_2(w) \leq a$ we get $H_2(w) = 0$.

So we have $c = H(w) = H_3(w) \wedge H_4(w) \wedge H_5(w) \wedge c$, and now:

$H_3(w) \geq c$, and with $H_3(w) \geq b$ we get $H_3(w) = 1$.
$H_4(w) \geq c$, and with $H_4(w) \geq b$ we get $H_4(w) = 1$.
$H_5(w) \geq c$, and with $H_5(w) \geq b$ we get $H_5(w) = 1$.

With Proposition 28 we obtain:

(1) $\forall i(1 \leq i \leq n) : w_i \wedge w_{n+i} \in \{0, c\}$, because $H_1(w) = 0$,
(2) $\forall i(1 \leq i \leq n) : w_i \wedge w_{n+i} \in \{0, b\}$, because $H_2(w) = 0$,
(3) $\forall i(1 \leq i \leq n) : w_i \in \{a, b, 1\}$, because $H_4(w) = 1$,
(4) $\forall i(1 \leq i \leq n) : w_{n+i} \in \{a, b, 1\}$, because $H_5(w) = 1$.

Putting together (1) and (2) we get $w_i \wedge w_{n+i} = 0$ and together with (3) and (4) we can define $y = (y_1, \ldots, y_n) \in \{0, 1\}^n$ by

$$\forall i(1 \leq i \leq n) : y_i =_{\mathrm{df}} \begin{cases} 1 & \text{if } (w_i, w_{n+i}) = (a, b), \\ 0 & \text{if } (w_i, w_{n+i}) = (b, a), \end{cases}$$

which holds: $w = w_y$. This means:

$$\{w \in \mathrm{V}_1^{2n} \mid H(w) = c\} \subseteq \{w_y \mid y \in \{0, 1\}^n\}.$$

On the other hand it is easy to verify $H(w_y) = c \Leftrightarrow F(y) = 1$. So we have

$$\{w \in \mathrm{V}_1^{2n} \mid H(w) = c\} = \{w_y \mid F(y) = 1\},$$

which means $\#_{\mathrm{V}_1}^{c}(H) = \#3\mathrm{SAT}(F)$.

So the counting problem $\#_{\mathrm{V}_1}^{c}$ is not only $\leq_{1-T}^{log}$-complete for #P, as showen in Theorem 7. The counting problem $\#_{\mathrm{V}_1}^{c}$ is $\leq_{m}^{log}$-complete for #P as well.