The Inference Problem for Propositional Circumscription of Affine Formulas is coNP-complete

Arnaud Durand[1] and Miki Hermann[2]

[1] LACL Paris 12 and LAMSADE Paris 9 (CNRS UMR 7024), Dept. of Computer Science, Université Paris 12, 94010 Créteil, France. durand@univ-paris12.fr
[2] LIX (CNRS, UMR 7650), École Polytechnique, 91128 Palaiseau cedex, France. hermann@lix.polytechnique.fr

Abstract. We prove that the inference problem of propositional circumscription for affine formulas is coNP-complete, settling this way a longstanding open question in the complexity of nonmonotonic reasoning. We also show that the considered problem becomes polynomial-time decidable if only a single literal has to be inferred from an affine formula.

1 Introduction and Summary of Results

Various formalisms of nonmonotonic reasoning have been investigated during the last twenty-five years. Circumscription, introduced by McCarthy [McC80], is a well-developed formalism of common-sense reasoning extensively studied by the artificial intelligence community. It has a simple and clear semantics, and benefits from high expressive power, that makes it suitable for modeling many problems involving nonmonotonic reasoning. The key idea behind circumscription is that we are interested only in the *minimal models* of formulas, since they are the ones with as few "exceptions" as possible, and embody therefore common sense. Moreover, propositional circumscription inference has been shown by Gelfond *et al.* [GPP89] to coincide with reasoning under the extended closed world assumption, which is one of the main formalisms for reasoning with incomplete information. In the context of Boolean logic, circumscription amounts to the study of models of Boolean formulas that are *minimal* with respect to the *pointwise partial order* on models.

Several algorithmic problems have been studied in connection with propositional circumscription: among them the *model checking* and the *inference* problems. Given a propositional formula φ and a truth assignment s, the model checking problem asks whether s is a minimal model of φ. Given two propositional formulas φ and ψ, the inference problem asks whether ψ is true in every minimal model of φ. Cadoli proved in [Cad92] the model checking problem to be coNP-complete, whereas Kirousis and Kolaitis settled in [KK01a] the question of the dichotomy theorem for this problem. The inference problem was proved Π_2P-complete by Eiter and Gottlob in [EG93]. Cadoli and Lenzerini proved in [CL94] that the inference problem becomes coNP-complete if φ is a

Krom or a dual Horn formula. See also [CMM01] for an exhaustive overview of existing complexity results in nonmonotonic reasoning and circumscription. The complexity of the inference problem for affine formulas remained open for ten years. It was known that the problem is in coNP, but there was no proved coNP-hardness lower bound.

This paper is a partial result of our effort to find an output-polynomial algorithm for enumerating the minimal models of affine formulas, an open problem stated in [KSS00]. Following the result of Berlekamp *et al.* [BMvT78], it is clear that we cannot develop an output-polynomial algorithm for this enumeration problem by producing consecutive minimal models of the affine system with increasing Hamming weight, unless P = NP. Another natural approach consists of producing partial assignments to the variables that are extended to minimal models afterwards. However, as our result indicates, this new approach does not lead to an output-polynomial algorithm either, unless the same collapse occurs.

We settle in this paper the complexity of the inference problem for the propositional circumscription of affine formulas, proving that the problem is coNP-complete. First, we prove a new criterion for determining whether a given partial solution of an affine system can be extended to a minimal one. This criterion, which is interesting on its own, is then extensively used in the subsequent coNP-hardness proof of the inference problem for affine formulas. More precisely, we prove the NP-hardness of the problem, given a partial solution s of an affine system S, whether it can be extended to a minimal solution $\bar{s}$. To our knowledge, this proof uses a new approach combining matroid theory, combinatorics, and computational complexity techniques. The inference problem for affine circumscription is then the dual problem to minimal extension, what proves the former to be coNP-complete. Finally, we prove that the restriction of the affine inference problem with ψ being a single literal is decidable in polynomial time.

2 Preliminaries

Let $s = (s_1, \ldots, s_n)$ and $s' = (s'_1, \ldots, s'_n)$ be two Boolean vectors from $\{0,1\}^n$. We write $s < s'$ to denote that $s \neq s'$ and $s_i \leq s'_i$ holds for every $i \leq n$. Let $\varphi(x_1, \ldots, x_n)$ be a Boolean formula having $x_1, \ldots, x_n$ as its variables and let $s \in \{0,1\}^n$ be a truth assignment. We say that s is a *minimal model* of φ if s is a satisfying truth assignment of φ and there is no satisfying truth assignment s' of φ that satisfies the relation $s' < s$. This relation is called the *pointwise partial order* on models.

Let $\varphi(x_1, \ldots, x_n)$ be a propositional formula in conjunctive normal form. We say that $\varphi(x)$ is *Horn* if φ has at most one positive literal per clause, *dual Horn* if φ has at most one negative literal per clause, *Krom* if φ has at most two literals per clause, and *affine* if φ is a conjunction of clauses of the type $x_1 \oplus \cdots \oplus x_n = 0$ or $x_1 \oplus \cdots \oplus x_n = 1$, where $\oplus$ is the exclusive-or logical connective, what is equivalent to an affine system of equations $S\colon Ax = b$ over $\mathbb{Z}_2$.

Let φ and ψ be two propositional formulas in conjunctive normal form. We say that ψ follows from φ in propositional circumscription, denoted by $\varphi \models_{\min} \psi$, if ψ is true in every minimal model of φ. Since ψ is a conjunction $c_1 \wedge \cdots \wedge c_k$ of clauses c_i, then $\varphi \models_{\min} \psi$ if and only if $\varphi \models_{\min} c_i$ for each i. Hence we can restrict ourselves to consider only a single clause instead of a formula ψ at the right-hand side of the propositional inference problem $\varphi \models_{\min} c$. We can further restrict the clause c to one containing only negative literals $c = \neg u_1 \vee \cdots \vee \neg u_n$, as it was showed in [KK01b].

If x and y are two vectors, we denote by $z = xy$ the vector obtained by concatenation of x and y. Let $S\colon Az = b$ be a $k \times n$ affine system of equations over $\mathbb{Z}_2$. Without loss of generality, we assume that the system S is in standard form, i.e., that the matrix A has the form $(I\ B)$, where I is the $k \times k$ identity matrix and B is an arbitrary $k \times (n-k)$ matrix of full column rank. For convenience, we denote by x the variables from z associated with I and by y the ones associated with B. Hence, we consider affine systems of the form $S\colon (I\ B)(xy) = b$.

If A is a $k \times n$ matrix, we denote by $A(i,j)$ the element of A positioned at row i and column j. The vector forming the row i of the matrix A is denoted by $A(i,-)$, whereas the column vector j of A is denoted by $A(-,j)$. Let $I \subseteq \{1,\ldots,k\}$ and $J \subseteq \{1,\ldots,n\}$ be two index sets. Then $A(I,-)$ denotes the submatrix of A restricted to the rows I. Similarly, $A(-,J)$ is then the submatrix of A restricted to the columns J, whereas $A(I,J)$ stands for the submatrix of A restricted to the rows I and columns J. There are also two matrices with a special notation: the $k \times k$ identity matrix I_k and the $k \times n$ all-zero matrix O_k^n.

For a $k \times n$ affine system $S\colon Az = b$ over $\mathbb{Z}_2$, an index set $J = \{j_1,\ldots,j_m\} \subseteq \{1,\ldots,n\}$ of cardinality $|J| = m$, and a Boolean vector $v = (v_1,\ldots,v_m)$ of length m, we denote by $S[J/v]$ the new system $S'\colon A'z' = b'$ formed by replacing each variable z_{j_i} by the value v_i. We also denote by $\mathit{one}(v) = \{i \mid v_i = 1\}$ and $\mathit{zero}(v) = \{i \mid v_i = 0\}$ the positions in the vector v assigned to the values 1 and 0, respectively. The Hamming weight $\mathit{wt}(v)$ of a vector v is equal to the cardinality of the set $\mathit{one}(v)$, i.e., $\mathit{wt}(v) = |\mathit{one}(v)|$.

Each affine system $S\colon Az = b'$ can be transformed to the standard form $(I\ B)(xy) = b$ by means of Gaussian elimination in polynomial time. without changing the ordering of solutions. Indeed, a row permutation or addition does not change the solutions of S. A column permutation permutes the variables and therefore also the positions in each solution uniformly. However, for each column permutation π and a couple of solutions s, s', the relation $s < s'$ holds if and only if $\pi(s) < \pi(s')$. This allows us to consider affine systems in the form $S\colon (I\ B)(xy) = b$ without loss of generality.

Suppose that s is a variable assignment for the variables y, i.e., for each $y_i \in y$ there exists a value $s(y_i) \in \mathbb{Z}_2$. The vector s is a *partial assignment* for variables $z = xy$. An *extension* of the vector s is a variable assignment $\bar{s}$ for each variable from z, i.e., for each $z_i \in z$ there exists a value $\bar{s}(z_i) \in \mathbb{Z}_2$, such that $s(y_i) = \bar{s}(y_i)$ for each y_i. If s is a variable assignment for the variables y in the affine system $S\colon (I\ B)(xy) = b$ then the extension $\bar{s}$ to a solution of the system S is *unique*. If the variables y in the system $S\colon (I\ B)(xy) = b$ have been assigned, then the values for the variables x are already determined. In connection with the previous notions we define the following two **index sets**

$$eq(s) = \{i \mid (Bs)_i = b_i\} \qquad \text{and} \qquad neq(s) = \{i \mid (Bs)_i \neq b_i\},$$

where $b = (b_1, \ldots, b_k)$ and $(Bs)_i$ means the i-th position of the vector obtained after multiplication of the matrix B by the vector s. The set $eq(s)$ (resp. $neq(s)$) is the subset of row indices i for which the unique extension $\bar{s}$ satisfies the equality $\bar{s}(x_i) = 0$ (resp. $\bar{s}(x_i) = 1$). It is clear that $eq(s) \cap neq(s) = \emptyset$ and $eq(s) \cup neq(s) = \{1, \ldots, k\}$ hold for each s.

3 A New Criterion For Affine Minimality

There exists a straightforward method to determine in polynomial time whether a solution s is minimal for an affine system S over $\mathbb{Z}_2$. However, this method is unsuitable for testing whether a partial solution s can be extended to a minimal solution $\bar{s}$ of S. We propose here a completely new method well-suited to decide whether an extension $\bar{s}$ is a minimal solution of S.

Proposition 1. *Let $S\colon (I\ B)(xy) = b$ be an affine $k \times n$ system over $\mathbb{Z}_2$ and let s be a Boolean vector of length $n - k$. The extension $\bar{s}$ is a minimal solution of S if and only if $B(eq(s), one(s))$ is a matrix of column rank $wt(s)$, i.e., all its columns are linearly independent.*

Proof. Suppose that $\bar{s}$ is minimal and the matrix $B(eq(s), one(s))$ has the column rank smaller than $wt(s)$. This means that the columns of $B(eq(s), one(s))$ are linearly dependent, therefore there exists a subset $J \subseteq one(s)$, such that $\sum_{j \in J} B(eq(s), j) = \mathbf{0}$ holds. Let t be a Boolean vector satisfying the condition $one(t) = one(s) \smallsetminus J$. The columns of the matrix $B(eq(s), one(s))$ can be partitioned into two sets: those in J and those in $one(t)$. Knowing that the columns in J add up to the zero vector $\mathbf{0}$, we derive the following equality.

$$\sum_{j \in one(s)} B(eq(s), j) = \sum_{j \in one(t)} B(eq(s), j) + \sum_{j \in J} B(eq(s), j) = \sum_{j \in one(t)} B(eq(s), j)$$

The vector t is smaller than s in the pointwise order. We will show that also the extensions $\bar{s}$ and $\bar{t}$ satisfy the relation $\bar{t} < \bar{s}$. For each row $i \in eq(s)$, the coefficients $B(i, j)$ sum up to the value b_i, i.e., that $\sum_{j \in one(s)} B(i, j) = \sum_{j \in one(t)} B(i, j) = b_i$. Recall that each variable in the vector x occurs in the system S exactly once, because of the associated identity matrix I_k. Since already the assignments s and t to the variables y sum up to the value b_i, this determines the value of the variable x_i in the extensions $\bar{s}$ and $\bar{t}$ to be $\bar{s}(x_i) = \bar{t}(x_i) = 0$ for each row $i \in eq(s)$. In the same spirit, the assignment s to the variables y sums up to the value $1 - b_i$ for each row $i \in neq(s)$, what determines the value of the variable x_i in the extension $\bar{s}$ to be $\bar{s}(x_i) = 1$. Therefore we have $\bar{t}(x_i) \leq \bar{s}(x_i) = 1$ for each row $i \in neq(s)$. This shows that $\bar{t}$ is a solution of S smaller than $\bar{s}$, what contradicts our assumption that $\bar{s}$ is minimal.

Conversely, suppose that the matrix $B(eq(s), one(s))$ has the column rank $wt(s)$ but $\bar{s}$ is not minimal. The latter condition implies that there exists a variable assignment t, such that the extension $\bar{t}$ is a solution of S satisfying the relation $\bar{t} < \bar{s}$. Let $J = one(\bar{s}) \smallsetminus one(\bar{t})$ be the set of positions on which the extensions $\bar{s}$ and $\bar{t}$ differ. Both extensions $\bar{s}$ and $\bar{t}$ are solutions of S, therefore we have $(I\ B)\bar{s} + (I\ B)\bar{t} = \sum_{j \in J}(I\ B)(-, j) = \mathbf{0}$. The index set J can be partitioned into two disjoint sets J_1 containing the positions smaller or equal to k, that are associated with the identity matrix I, and the set J_2 containing the positions greater than k, that are associated with the matrix B. Hence the inclusion $J_2 \subseteq one(s)$ holds. The columns of the identity matrix I are linearly independent, therefore the set J_2 must be nonempty in order to get the above sum equal to $\mathbf{0}$. The partition of J implies the equality $\sum_{j \in J_1} I(-, j) + \sum_{j \in J_2} B(-, j) = \mathbf{0}$. The restriction of this equality to the rows in $eq(s)$ yields $\sum_{j \in J_1} I(eq(s), j) + \sum_{j \in J_2} B(eq(s), j) = \mathbf{0}$. The vector $\bar{s}$ is a solution of S and for each row $i \in eq(s)$ we have $\bar{s}(x_i) = 0$, since already the values $s(y_j)$ with $j \in J_2$ sum up to b_i. This implies together with the previous equation that $i \notin J_1$, since $i \leq k$ holds, and for all indices $j \in J_1$ the column $I(eq(s), j)$ is the all-zero vector. This yields the equality $\sum_{j \in J_1} I(eq(s), j) = \mathbf{0}$, what implies the final equality $\sum_{j \in J_2} B(eq(s), j) = \mathbf{0}$. Since J_2 is a subset of the columns $one(s)$, this contradicts the fact that the matrix $B(eq(s), one(s))$ has the column rank $wt(s)$. ☐

4 Extension and Inference Problems

In this paper we will be interested in the complexity of the inference problem of propositional circumscription with affine formulas. Since affine propositional formulas are equivalent to affine systems $S\colon Az = b$ over $\mathbb{Z}_2$, this problem can be formulated as follows.

Problem: AFFINF
Input: An affine system $S\colon Az = b$ over $\mathbb{Z}_2$ with a Boolean $k \times n$ matrix A, a Boolean vector b of length k, a variable vector $z = (z_1, \ldots, z_n)$, and a negative clause $c = \neg u_1 \vee \cdots \vee \neg u_m$, where $u_i \in z$ holds for each i.
Question: Does $S \models_{\min} c$ hold?

Another interesting problem, closely related to the previous one, is the problem of extending a Boolean vector to a minimal solution of an affine system.

Problem: MINEXT
Input: An affine system $S\colon Az = b$ over $\mathbb{Z}_2$ with a Boolean $k \times n$ matrix A, a Boolean vector b of length k, a variable vector $z = (z_1, \ldots, z_n)$, and a partial assignment s for the variables y, where $z = xy$.
Question: Can s be extended to a vector $\bar{s}$, such that $\bar{s}$ is a minimal solution of the system S?

The minimal extension problem appears naturally within algorithms enumerating minimal solutions. For any given class of propositional formulas, when the corresponding minimal extension problem is polynomial-time decidable, then there exists an algorithm that enumerates each consecutive pair of minimal solutions with polynomial delay.

To derive the lower bound of the complexity of the latter problem, we need to consider the following well-known NP-complete problem.

Problem: POSITIVE 1-IN-3 SAT
Input: A propositional formula φ in conjunctive normal form with three positive literals per clause.
Question: Is there a truth assignment to the variable of φ, such that exactly one literal is assigned to *true* and the two others are assigned to *false* in every clause?

Theorem 2. MINEXT *is* NP*-complete even if the partial assignment s contains no 0.*

Proof. Membership of MINEXT in NP is obvious. For the lower bound, we construct a polynomial reduction from the problem POSITIVE 1-IN-3 SAT.

Let $\varphi(x_1,\ldots,x_n)$ be a propositional formula in conjunctive normal form $c_1 \wedge \cdots \wedge c_m$ with the clauses $c_i = x_i^1 \vee x_i^2 \vee x_i^3$. We construct an affine system $S\colon (I\ B)(zxy) = b$, where I is the $(4m+n)\times(4m+n)$ identity matrix, z, x, and y are variable vectors of respective lengths $4m+n$, n, and $3m$, and B is a special $(4m+n)\times(3m+n)$ matrix encoding the formula φ. We also construct a partial assignment s and show that the formula φ has a model satisfying exactly one variable per clause if and only if s can be extended to a minimal solution of S.

The matrix B is composed from six blocks as follows

$$\begin{pmatrix} B_1^1 & B_1^2 \\ B_2^1 & B_2^2 \\ B_3^1 & B_3^2 \end{pmatrix}$$

The matrix B_1^1 of size $m \times n$ is the clause-variable incidence matrix of the formula φ, i.e., $B_1^1(i,j) = 1$ holds if and only if $x_j \in c_i$. The matrix B_1^2 of size $m \times 3m$ is the identity matrix I_m with each column tripled, i.e., it verifies the conditions $B_1^2(i, 3(i-1)+1) = B_1^2(i, 3(i-1)+2) = B_1^2(i, 3i) = 1$ for all i and $B_1^2(i,j) = 0$ otherwise. The matrix B_2^1 of size $3m \times n$ encodes the polynomials $x_i^1 + x_i^2$, $x_i^2 + x_i^3$, and $x_i^3 + x_i^1$ over $\mathbb{Z}_2$ for each clause $c_i = x_i^1 \vee x_i^2 \vee x_i^3$. This encoding is done for each $i = 1,\ldots,m$ in three consecutive rows. Hence, we have $B_2^1(3i, i_1) = B_2^1(3i, i_2) = 1$, $B_2^1(3i+1, i_2) = B_2^1(3i+1, i_3) = 1$, and $B_2^1(3i+2, i_3) = B_2^1(3i+2, i_1) = 1$, where i_j is the position of the variable x_i^j in the vector $x = (x_1,\ldots,x_n)$. Otherwise we have $B_2^1(3i+q, j) = 0$ for $q = 0,1,2$ and $j \neq i_1, i_2, i_3$. In another words, the rows $B_2^1(3i,-)$, $B_2^1(3i+1,-)$, and $B_2^1(3i+2,-)$ are the incidence vectors of the polynomials $x_i^1 + x_i^2$, $x_i^2 + x_i^3$, and $x_i^3 + x_i^1$, respectively. The matrix B_2^2 of size $3m \times 3m$ is the identity matrix I_{3m}. The matrix B_3^1 of size $n \times n$ is the identity matrix I_n, whereas the matrix B_3^2 of size $n \times 3m$ is the all-zero matrix O_n^{3m}. Note that due to the blocks B_2^2 and B_3^1, that are identity matrices, as well as the block B_3^2 that is an all-zero matrix, the matrix B has the column rank $n + 3m$. Denote by B_1 the submatrix of B restricted to the first m rows, i.e., $B_1 = B(\{1,\ldots,m\},-)$. Analogously, we define

$B_2 = B(\{m+1,\ldots,4m\},-)$ and $B_3 = B(\{4m+1,\ldots,4m+n\},-)$. In the same spirit, we denote by $B^1 = B(-,\{1,\ldots,n\})$ and $B^2 = B(-,\{n+1,\ldots,n+3m\})$ the left and the right part of the columns, respectively, of the matrix B.

The vector b of length $4m+n$ in the system S is a concatenation of three vectors b_1, b_2, and b_3, where b_1 is the all-zero vector of length m, b_2 is the all-zero vector of length $3m$, and b_3 is the all-one vector of length m. The parts b_i of the vector b correspond to the row blocks B_i of the matrix B for $i = 1,2,3$. Figure 1 describes the constructed matrix B and vector b.

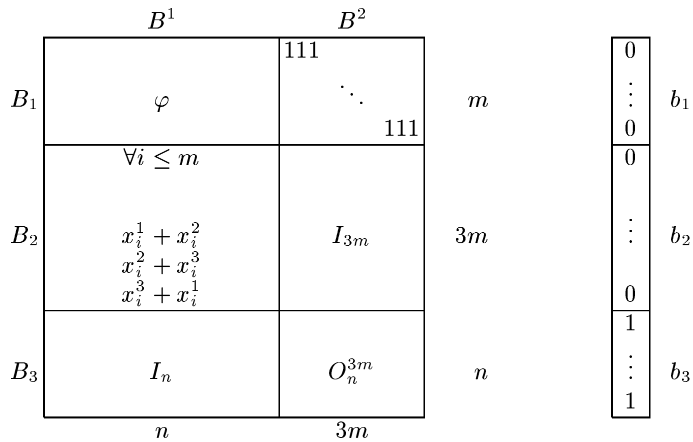

Fig. 1. Matrix B and the associated vector b

Finally, we set the vector s of size $3m$ to be equal to 1 in each coordinate, i.e., $s(y_i) = 1$ for each $i = 1,\ldots,3m$ and the Hamming weight of s is $wt(s) = 3m$.

Let v be a model of the formula φ satisfying exactly one literal per clause. We will prove that when we append the all-one vector s to v, forming the vector $t = vs$, then the extension $\bar{t}$ is a minimal solution of S. Let us study the set $eq(t)$. Since every clause $c_i = x_i^1 \vee x_i^2 \vee x_i^3$ of φ is satisfied, the sum of literal values is equal to $v(x_i^1) + v(x_i^2) + v(x_i^3) = 1$. Moreover, for each $j = 1,\ldots,m$ we have $s(x_j) = 1$, therefore all m rows of B_1 belong to $eq(t)$. Exactly two of the polynomials $x_i^1 + x_i^2$, $x_i^2 + x_i^3$, and $x_i^3 + x_i^1$ are evaluated to 1 for each clause c_i and for each $j = 1,\ldots,3m$ we have $s(x_j) = 1$, what implies that exactly $2m$ rows from B_2 belong to the set $eq(t)$. The row i of B_1 and the rows $3(i-1)+1$, $3(i-1)+2$, and $3i$ of B_2 correspond to the clause c_i. Form the corresponding row index set $I(i) = \{i,\ m+3(i-1)+1,\ m+3(i-1)+2,\ m+3i\}$ for a given i. Consider the restriction of the block B^2 to the rows $I(i)$. This restriction $B^2(I(i),-)$ will have plenty of all-zero columns. Keep only the columns containing at least one value 1. These columns will be $3(i-1)+1$, $3(i-1)+2$, and $3i$. Form the corresponding column index set $J(i) = \{n+3(i-1)+1,\ n+3(i-1)+2,\ n+3i\}$

for a given i. The restriction of B to the rows $I(i)$ and columns $J(i)$ is the matrix

$$B(I(i), J(i)) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = B^*(i).$$

Note that the first row of $B^*(i)$ and exactly two out of the three last rows of $B^*(i)$ are also represented in the set $eq(t)$. If we delete one of the last three rows of $B^*(i)$, the resulting square matrix will remain non-singular. Note that the column index sets $J(i)$ are pairwise disjoint and that their union equals the index set $J^* = \{n+1, \dots, n+3m\}$. Since $B(-, J^*) = B^2$ holds, we easily see that the restriction $B^2(\{1, \dots, 4m\}, -)$ is equal, modulo a suitable row permutation, to the block matrix

$$B^2_{1+2} = \begin{pmatrix} B^*(1) & O & O \\ O & \ddots & O \\ O & O & B^*(m) \end{pmatrix}.$$

The restriction $B^2(eq(t), -)$ deletes from B^2_{1+2} one of the last three rows of each block corresponding to $B^*(i)$. The matrix B^2_{1+2} is non-singular, what implies that the restriction $B^2(eq(t), -)$ is also non-singular, since $B^*(i)$ with one row deleted remains non-singular. Finally, the block B_3 contributes $wt(v)$ rows to $eq(t)$. Hence, the set $eq(t)$ contains $3m + wt(v)$ row indices and the equality $wt(t) = 3m + wt(v)$ holds. This means that $B(eq(t), one(t))$ is a square matrix. Note that $B(eq(t), one(t))$ is the concatenation of the matrices $B(eq(t), one(v))$ and $B(eq(t), one(s))$, since $t = vs$. Because s is the all-one vector, the matrix $B(eq(t), one(s))$ is equal to $B^2(eq(t), -)$. Notice that $B(eq(t) \cap \{4m+1, \dots, 4m+n\}, one(v))$ (i.e. the restriction of $B^1(eq(t), one(v))$ to rows of B^1_3) is once more an identity matrix, what makes the block $B^1(eq(t), one(v)) = B(eq(t), one(v))$ non-singular. Finally, the block B^2_3 is an all-zero matrix, therefore the concatenation of matrices $B(eq(t), one(v)) B(eq(t), one(s)) = B(eq(t), one(t))$ is non-singular, what means that its columns are linearly independent. According to Proposition 1, the extension $\bar{t}$ is a minimal solution of S, hence s can be extended to a minimal solution of the system S.

Conversely, suppose that s can be extended to a minimal solution of S. Then there exists a partial assignment v to the variables x, forming with s the concatenation $t = vs$, such that $\bar{t}$ is minimal and $wt(t) = 3m + wt(v)$ holds. Note that independently from the choice of the values $v(x_i^1)$, $v(x_i^2)$, and $v(x_i^3)$, at most two of the polynomials $x_i^1 + x_i^2$, and $x_i^2 + x_i^3$, and $x_i^3 + x_i^1$ evaluate to 1. Hence, at most $2m$ rows of B_2 are evaluated to 0 by the assignment t.

Let us analyze the row indices of B that belong to $eq(t)$. The block B_2 contributes always at most $2m$ elements and the block B_3 contributes exactly $wt(v)$ elements to $eq(t)$. Suppose that not all indices of B_1 belong to $eq(t)$. In this case, the block B_1 contributes at most $m - 1$ elements to $eq(t)$. This implies that the cardinality of the set $eq(t)$ is smaller or equal than $3m - 1 + wt(v)$ and

$B(eq(t), one(t))$ is a $(3m - 1 + wt(v)) \times (3m + wt(v))$ matrix. In this case the column rank of the matrix $B(eq(t), one(t))$ is smaller than $3m + wt(v)$, i.e., the columns are linearly dependent. Following Proposition 1, the extension $\bar{t}$ cannot be minimal. Hence, all m row indices of B_1 must belong to $eq(t)$.

Since all m rows of B_1 belong to $eq(t)$ and $s(y_j) = 1$ holds for each j, the structure of B_1^1, encoding the clauses $c_i = x_i^1 \vee x_i^2 \vee x_i^3$ of φ, implies that the equality $t(x_i^1) + t(x_i^2) + t(x_i^3) = v(x_i^1) + v(x_i^2) + v(x_i^3) = 1$ holds over $\mathbb{Z}_2$ for each i. There are two cases to analyze: (1) either $v(x_i^1) = v(x_i^2) = v(x_i^3) = 1$ or (2) exactly one of the values $v(x_i^1)$, $v(x_i^2)$, $v(x_i^3)$ is equal to 1 and the two others are equal to 0. Suppose that there exists an i such that Case 1 is satisfied. Then the maximal number of row indices in $eq(t)$ contributed by B_2 is $2(m-1)$. This is because the equalities $v(x_i^1) + v(x_i^2) = v(x_i^2) + v(x_i^3) = v(x_i^3) + v(x_i^1) = 0$ hold over $\mathbb{Z}_2$. The cardinality of $eq(t)$ is then bounded by $3m - 2 + wt(v)$, what implies once more that the columns of $B(eq(t), one(t))$ are linearly dependent and this leads to the same contradiction, implying that the extension $\bar{t}$ is not minimal, as in the previous paragraph. Case 2 presents a valid 1-in-3 assignment to φ. □

Theorem 3. *The problem* AFFINF *is* coNP*-complete.*

Proof. The problem AFFINF is the dual of the problem MINEXT. Note that, given a formula φ and a clause $c = \neg u_1 \vee \cdots \vee \neg u_k$, the condition $\varphi \models_{\min} \neg u_1 \vee \cdots \vee \neg u_k$ holds if and only if there is no minimal model m of φ that satisfies $m(u_1) = \cdots = m(u_k) = 1$. The latter is true if and only if the partial assignment s with $s(u_1) = \cdots = s(u_k) = 1$ cannot be extended to a minimal model of φ, or equivalently, to a minimal solution of the affine system S corresponding to φ. □

5 Decompositions and Polynomial-time Decidable Cases

Eiter and Gottlob proved in [EG93] that the inference problem $\varphi \models_{\min} c$ for propositional circumscription remains Π_2P-complete even if the clause c consists of a single negative literal $\neg u$. However, it is not guaranteed that the complexity remains the same for one-literal clauses c for the usual subclasses of propositional formulas. Concerning the considered inference problem, Cadoli and Lenzerini proved in [CL94] that for dual Horn formulas it remains coNP-complete but for Krom formulas it becomes polynomial-time decidable for a clause c consisting of a single negative literal. It is a natural question to ask what happens in the case of affine formulas in the presence of a single literal. In the rest of the section we will focus on the restrictions AFFINF_1 and MINEXT_1 of the respective problems AFFINF and MINEXT to a single negative literal clause $c = \neg u$.

To be able to investigate the complexity of MINEXT_1 and AFFINF_1, we need to define a neighborhood and a congruence closure on the columns.

Definition 4. *Let B be a $k \times n$ matrix over $\mathbb{Z}_2$ and let $j \in \{1, \ldots, n\}$ be a column index. The* ***p-neighborhood*** *$N_p(j)$ of the column j in B, for $p = 0, 1, \ldots, n$, is* *defined inductively by*

$$\begin{aligned} N_0(j) &= \{j\}, \\ N_{p+1}(j) &= \{m \mid (\forall q)[(q \leq p) \rightarrow (m \notin N_q(j))] \ \wedge \\ &\qquad\qquad (\exists \ell)(\exists i)[(\ell \in N_p(j)) \wedge (B(i,\ell) = B(i,m) = 1)]\}. \end{aligned}$$

The ***connected component*** $CC(j)$ *of the column* j *in* B *is the union of the* p*-neighborhoods for all* p*, i.e.,* $CC(j) = \bigcup_{p=0}^{n} N_p(j)$*.*

Speaking in terms of hypergraphs and matroids, where B is interpreted as the vertex-hyperedge incidence matrix, the p-neighborhood $N_p(j)$ is the set of vertices reachable from the vertex j by a path of length p. The vertex ℓ belongs to $N_p(j)$ if and only if the shortest path from j to ℓ in B has the length p. The connected component $CC(j)$ is the set of all reachable vertices from j.

Example 5. Consider the following following affine system $S\colon (I\ B)(xy) = b$, where I, B and b are represented by the successive blocks of the following matrix.

$$(I \mid B \mid b) = \left(\begin{array}{cccccc|ccccc|c} 1&0&0&0&0&0 & 0&1&\boxed{1}&\boxed{1}&0 & 0 \\ 0&1&0&0&0&0 & 1&0&0&0&0 & 0 \\ 0&0&1&0&0&0 & 1&1&1&0&0 & 0 \\ 0&0&0&1&0&0 & \boxed{1}&0&\boxed{1}&0&0 & 0 \\ 0&0&0&0&1&0 & 0&0&0&\boxed{1}&1 & 1 \\ 0&0&0&0&0&1 & 0&0&0&0&1 & 1 \end{array}\right)$$

Take $j = 7$ and compute the p-neighborhood from vertex 7 in the matrix B for each $p = 0, 1, \ldots, 6$. We obtain $N_0(7) = \{7\}$, $N_1(7) = \{8, 9\}$, $N_2(7) = \{10\}$, $N_3(7) = \{11\}$, and $N_4(7) = N_5(7) = N_6(7) = \emptyset$. The connected component of the vertex 7 is $CC(7) = \{7, 8, 9, 10, 11\}$.

When computing the connected component for all columns of a given matrix B, we may get two or more disjoint sets of vertices. In this case we say that the matrix B is *decomposable*. The following lemma shows that we can compute the problems MINEXT and AFFINF by connected components without increasing the complexity.

Lemma 6. *Let* $S\colon (I\ B)(xy) = b$ *be an affine system over* $\mathbb{Z}_2$*. Suppose that the matrix* B *can be decomposed, up to a permutation of rows and columns, into the components*

$$\begin{pmatrix} B_1 & O \\ O & B_2 \end{pmatrix}$$

where B_1 *is a* $k_1 \times n_1$ *matrix and* B_2 *is a* $k_2 \times n_2$ *matrix. Let* b_1 *and* b_2 *be two vectors of respective size* n_1 *and* n_2*, such that* $b = b_1 b_2$*. Then the set of minimal solutions of* S *is equal, up to a permutation, to the Cartesian product* $M_1 \times M_2$ *of the sets of minimal solutions* M_1 *and* M_2 *of the systems* $S_1\colon (I\ B_1)(x'y') = b_1$ *and* $S_2\colon (I\ B_2)(x''y'') = b_2$*, respectively, where* $x = x'x''$ *and* $y = y'y''$*.*

The proof of the following theorem shows that finding a minimal extension $\bar{s}$ of a Boolean vector s with $wt(s) = 1$ can be done by finding a shortest path in a connected component of the matrix B from a given column to an inhomogeneous equation in the system S.

Theorem 7. MINEXT$_1$ *and* AFFINF$_1$ *are decidable in polynomial time.*

Proof. (*Hint*) Suppose without loss of generality that S is a $k \times n$ system of the form $S\colon (I\ B)(xy) = b$ and that the variable assigned by s is y_1. This can be achieved through a suitable permutation of rows and columns. We also suppose that the matrix B is indecomposable. Otherwise, we could apply the method described in this proof to one of the subsystems S_1 or S_2 separately, following Lemma 6. Since B is indecomposable, the connected component of the first column is $CC(1) = \{1, \ldots, n\}$, i.e., there are no unreachable columns. The following condition holds for extensions of vectors with weight 1 to minimal solutions: There exists a minimal solution $\bar{s}$ with $\bar{s}(y_1) = 1$ if and only if $b \neq \mathbf{0}$.

If $b = \mathbf{0}$ then the system S is homogeneous and the all-zero assignment for xy is the unique minimal solution of S, what contradicts the existence of a minimal solution $\bar{s}$ with $\bar{s}(y_1) = 1$.

Conversely, suppose that $b \neq \mathbf{0}$. We construct a partial assignment s for the variables y with $s(y_1) = 1$, such that $\bar{s}$ is minimal. We must find the first inhomogeneous equation reachable from y_1. Since $b \neq \mathbf{0}$, there exists a shortest path through $p+1$ hyperedges $j_0 = 1, j_1, \ldots, j_p$ of the hypergraph corresponding to the matrix B, such that the following conditions hold: (1) each hyperedge j_q, $q \leq p$, is reachanble from j_0 since each pair of consecutive hyperedges j_q and j_{q+1} has a common vertex, (2) the existence of a vertex i in a hyperedge j_q, where $q < p$, implies $b_i = 0$, and (3) there exists a vertex i in the last hyperedge j_p, such that $b_i = 1$. Define the partial assignment s for the variables y by $s(y_{j_q}) = 1$ for each $q \leq p$ and set $s(y_j) = 0$ otherwise. This assignment corresponds to the shortest hyperpath starting from a vertex of the hyperedge j_0 and finishing in a vertex i of the hyperedge j_p, such that $b_i = 1$. It is easy to see that $\bar{s}$ is a minimal solution of S corresponding to the shortest hyperpath. Each vertex i_q, except the last one, occurs twice in the shortest hyperpath, what allows us to have $b_{i_q} = 0$. The last vertex i_p appears only once, what implies $b_{i_p} = 1$. The variables x are all set equal to 0. Both a shortest hyperpath and the connceted component can be computed in polynomial time, therefore both problems MINEXT$_1$ and AFFINF$_1$ are polynomial-time decidable. ☐

Example 8 (Example 5 continued). Start with the column $j_0 = 7$ and compute a shortest path reaching an inhomogeneous equation. There is a shortest path from the column 7 through the columns $j_0 = 7$, $j_1 = 9$, $j_2 = 10$, reaching the inhomogeneous row 5. The path $B(4,7) \to B(4,9) \to B(1,9) \to B(1,10) \to B(5,10)$ is indicated in the matrix by boxed values. Hence, we computed the partial assignment $s = (1,0,1,1,0)$ for the variables y and the extension $\bar{s} = (0,1,0,0,0,1,1,0,1,1,0)$ is a minimal solution of the system S.

6 Conclusion

formula φ	clause inference c	literal inference c
CNF	Π_2P-complete [EG93]	Π_2P-complete [EG93]
Horn	in P	in P
dual Horn	coNP-complete [CL94]	coNP-complete [CL94]
Krom	coNP-complete [CL94]	in P [CL94]
affine	coNP-complete [Theorem 3]	in P [Theorem 7]

Fig. 2. Complexity of the inference problem of propositional circumscription

We proved that the inference problem of propositional circumscription for affine formulas is coNP-complete. It also shows that reasoning under the extended closed world assumption is intractable for affine formulas. In fact, the exact complexity of affine inference was an open problem since the beginning of the 1990s when several researchers started to investigate the propositional circumscription from algorithmic point of view. We also proved that the inference problem for affine formulas becomes polynomial-time decidable when only a single literal has to be inferred. The complexity classification of the inference problem of propositional circumscription for the usual classes of formulas is presented in Figure 2.

References

[BMvT78] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. on Inf. Theory*, IT-24(3):384–386, 1978.

[Cad92] M. Cadoli. The complexity of model checking for circumscriptive formulae. *Inf. Proc. Letters*, 44(3):113–118, 1992.

[CL94] M. Cadoli and M. Lenzerini. The complexity of propositional closed world reasoning and circumscription. *JCSS*, 48(2):255–310, 1994.

[CMM01] S. Coste-Marquis and P. Marquis. Knowledge compilation for closed world reasoning and circumscription. *J. Logic and Comp.*, 11(4):579–607, 2001.

[EG93] T. Eiter and G. Gottlob. Propositional circumscription and extended closed-world reasoning are Π_2^p-complete. *TCS*, 114(2):231–245, 1993.

[GPP89] M. Gelfond, H. Przymusinska, and T. C. Przymusinski. On the relationship between circumscription and negation as failure. *Artificial Intelligence*, 38(1):75–94, 1989.

[KK01a] L. M. Kirousis and P. G. Kolaitis. The complexity of minimal satisfiability problems. In A. Ferreira and H. Reichel, (eds), *Proc. 18th STACS, Dresden (Germany)*, LNCS 2010, pp 407–418. Springer, 2001.

[KK01b] L. M. Kirousis and P. G. Kolaitis. A dichotomy in the complexity of propositional circumscription. In *Proc. 16th LICS, Boston (MA)*, pp 71–80. 2001.

[KSS00] D. J. Kavvadias, M. Sideri, and E. C. Stavropoulos. Generating all maximal models of a boolean expression. *Inf. Proc. Letters*, 74(3-4):157–162, 2000.

[McC80] J. McCarthy. Circumscription — A form of non-monotonic reasoning. *Artificial Intelligence*, 13(1-2):27–39, 1980.