DOI 10.1007/s10469-024-09771-0
Algebra and Logic, Vol. 63, No. 1, March, 2024
(Russian Original Vol. 63, No. 1, January-February, 2024)

THE LENGTH OF AN UNSATISFIABLE SUBFORMULA

A. V. Seliverstov

UDC 510.633

Keywords: *propositional logic, satisfiability, rank of matrix, binary solution.*

We find a bound for the length of a conjunction of some propositional formulas, for which every unsatisfiable formula contains an unsatisfiable subformula. In particular, this technique applies to formulas in conjunctive normal form with restrictions on the number of true literals within every elementary disjunction, as well as for 2-CNFs, for symmetric 3-CNFs, and for conjunctions of voting functions in three literals. A lower bound on the rank of some matrices is used in proofs.

INTRODUCTION

A propositional conjunctive normal form (CNF) is a conjunction of elementary disjunctions each of which contains just literals. A literal is a propositional variable or the negation of a variable. If each elementary disjunction has k literals, then such a CNF is called a k-CNF. By $\perp$ and $\top$ we denote Boolean constants: the truth and the falsity respectively.

For two numbers $\alpha < \beta$, the set α-or-β-in-SAT consists of CNFs for which there exists a $(\perp, \top)$-valuation of variables such that in every elementary disjunction exactly α or exactly β literals turn out to be true. For $k < \alpha < \beta$, the set α-or-β-in-SAT does not contain a k-CNF. For $k < \beta$, some k-CNF φ belongs to the set 1-or-β-in-SAT iff φ belongs to a set 1-in-k-SAT consisting of k-CNFs for which there exists a $(\perp, \top)$-valuation of variables such that every elementary disjunction has exactly one literal true. Some 2-CNF φ belongs to the set 1-or-2-in-SAT iff φ is satisfiable. Some 3-CNF φ belongs to the set 1-or-2-in-SAT iff φ belongs to a set NAE-3-SAT. The latter set consists of those 3-CNFs for which there exists a $(\perp, \top)$-valuation of variables such that in every disjunction some literal is false and some literal is true. The belonging of a 3-CNF $\varphi(p_1, \ldots, p_n)$ to

Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, Russia; SLVSTV@iitp.ru. Translated from *Algebra i Logika*, Vol. 63, No. 1, pp. 89-99, January-February, 2024. Russian DOI: 10.33048/alglog.2024.63.107. Original article submitted December 15, 2023; accepted December 4, 2024.

NAE-3-SAT is equivalent to the satisfiability of a formula $\varphi(p_1, \ldots, p_n) \wedge \varphi(\neg p_1, \ldots, \neg p_n)$. Both the problems recognizing the belonging of a 3-CNF to NAE-3-SAT and to 1-in-3-SAT are, as is known, NP-complete. Length of a formula serves as a natural parameter for estimating the computational complexity (see [1, 2]). In [3], an algorithm is offered for verifying the satisfiability of CNF, whose running time on CNF in n variables with $m > n$ elementary disjunctions is upper bounded by the function $O(2^{m-n}n^3)$. In particular, the running time is polynomially bounded for a fixed difference $m - n$ but grows exponentially for $m > 2n$. It is of interest, therefore, whether it is possible to replace an initial 3-CNF by a subformula. Certain results are known that limit the possibility of such a replacement not only in the worst case but also in the general case.

We fix an arbitrarily small $\varepsilon > 0$. Almost all 2-CHFs in n variables, the number of elementary disjunctions in which is less than a threshold $(1-\varepsilon)n$, are satisfiable. On the contrary, unsatisfiable are almost all 2-CNFs in n variables the number of elementary disjunctions in which is greater than a threshold $(1+\varepsilon)n$ (see [4, 5]). Existence of such a threshold is usually called a phase transition and is exemplified in [6] on random samples of formulas of several types.

If every elementary disjunction contains precisely k literals and every variable occurs in exactly d elementary disjunctions, then a k-CNF is said to be d-regular. For any sufficiently large number k, the belonging of a random d-regular k-CNF to the set NAE-k-SAT undergoes with growing d a phase transition for some critical value d_k, which depends on k. As the number of variables grows, a share of d-regular k-CNFs belonging to NAE-k-SAT tends to one for $d < d_k$ and tends to zero for $d > d_k$ (see [7]). A similar result for d-regular k-CNFs in which, under some valuation, exactly two literals in each elementary disjunction are true was obtained in [8].

In proofs, we replace a CNF by a system of algebraic equations depending on auxiliary variables, one for each elementary disjunction. The initial satisfiability problem for CNF reduces to the incidence problem for a subspace defined by a system of linear equations, and point sets with coordinates from the set $\{0, 1\}$. Related incidence problems for lines and points were considered in [9, 10]. From a geometrical viewpoint, eliminating from CNF an elementary disjunction corresponds to a projection onto some coordinate subspace. This projection corresponds to the elimination of an auxiliary variable. Such an approach applies not only to CNFs but to other formulas as well. Usually, with Boolean formulas we associate equations over a field of two elements (see [11]). However, likewise we can consider systems of equations over other fields. A solution to a system of equations in which each variable assumes values from the set $\{0, 1\}$ is called a $(0, 1)$-solution. Searching a $(0, 1)$-solution for a system of linear equations over the field of rationals is a well-known computationally hard problem (see [12]).

The paper consists of three sections. Preliminary information is given in Sec. 1 where lemmas from linear algebra are collected and will then be used in Sec. 2 in proving two theorems. Examples and remarks are discussed in Sec. 3.

1. PRELIMINARY INFORMATION

We denote by K a field consisting of at least three elements. Let a system of linear equations in variables $x_1, \ldots, x_n$ contain more than one equation and suppose that some equation nontrivially depends on a variable x_k. A new system of linear equations is obtained from the initial system by deleting the variable x_k if the new system does not depend on x_k, and the initial system is equivalent to a combination of the new system and precisely one equation (depending on x_k), equal to a linear combination of the equations in the initial system.

We consider an affine space over a field K with a fixed system of Cartesian coordinates. The rank of a square matrix M is associated with the dimension of an affine envelope L of points corresponding to columns of the matrix. If L contains the origin of coordinates, then $\operatorname{rank}(M) = \dim(L)$, and otherwise $\operatorname{rank}(M) = \dim(L) + 1$.

Point in an affine space each coordinate of which is equal to zero or one is called a $(0,1)$-point. Replacement of the coordinate x_k by the difference $1 - x_k$ maps a $(0,1)$-point to another $(0,1)$-point. Whereas the dimension of any subspace remains unchanged.

LEMMA 1. An $n \times n$ matrix M over a field K is such that each of its elements on the principal diagonal is distinct from zero and one, while each element outside the principal diagonal is equal either to zero or to one. Then the rank of the matrix M is at least $n/2$.

Proof. If $n = 2$, then the rank of a 2×2 matrix M is not less than a number $n/2$ since $\operatorname{rank}(M) \geqslant 1$. Suppose that, for some $n \geqslant 3$, the lemma has already been proven for all square matrices of lesser order to be treated, and consider the $n \times n$ matrix M.

Transformation $x_k \to 1 - x_k$ means that all elements in the kth row of the matrix will be replaced. Applying these transformations, we may pass from matrix M to matrix $\hat{M}$ of the same type, but in the last column of $\hat{M}$ all elements except one on the principal diagonal are equal to zero. We have a matrix

$$\hat{M} = \left(\begin{array}{ccc|c} & & & 0 \\ & N & & \vdots \\ & & & 0 \\ \hline * & \cdots & * & c \end{array}\right)$$

for some $c \notin \{0, 1\}$. The affine envelopes of columns in both matrices M and $\hat{M}$ have equal dimensions. Therefore, $\operatorname{rank}(M) \geqslant \operatorname{rank}(\hat{M}) - 1$. But if the affine envelope of columns in M contains the origin of coordinates, then the rank of M may be less than that of $\hat{M}$.

Performing elementary transformations with columns of matrix $\hat{M}$ yields a matrix

$$\widetilde{M} = \left(\begin{array}{ccc|c} & & & 0 \\ & N & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & c \end{array}\right)$$

of the same rank. Only bottom rows of $\hat{M}$ and $\widetilde{M}$ may be different. In the bottom row of $\widetilde{M}$, all elements except one on the principal diagonal are zeros. Removing the last column and the last row from the matrix $\widetilde{M}$ yields an $(n-1)\times(n-1)$ matrix N of lesser rank. By the induction hypothesis, $\mathrm{rank}(N) \geqslant (n-1)/2$. Therefore, the inequality $\mathrm{rank}(\widetilde{M}) \geqslant (n+1)/2$ holds.

We denote by L the affine envelope of columns in matrix $\widetilde{M}$. If L passes through the origin of coordinates then $\mathrm{rank}(\widetilde{M}) = \dim(L)$. In this case $\mathrm{rank}(M) \geqslant \dim(L) = \mathrm{rank}(\widetilde{M}) \geqslant (n+1)/2$.

If, however, the subspace L does not pass through the origin, then $\mathrm{rank}(M) \geqslant \mathrm{rank}(\widetilde{M}) - 1 = \mathrm{rank}(N)$. In this case the affine envelope of columns in matrix N does not pass through the origin. If again we apply transformations like $x_k \to 1 - x_k$ to the matrix N we obtain a matrix

$$\widetilde{N} = \left(\begin{array}{ccc|c} & & & 0 \\ & W & & \vdots \\ & & & 0 \\ \hline * & \cdots & * & * \end{array}\right)$$

of the same form, but in the last column of $\widetilde{N}$ all elements except one on the principal diagonal are equal to zero. Moreover, since the affine envelope of columns of matrix N does not pass through the origin of coordinates, the inequality $\mathrm{rank}(N) \geqslant \mathrm{rank}(\widetilde{N})$ holds. Removing from $\widetilde{N}$ the last column and the last row, we obtain an $(n-2)\times(n-2)$ matrix W of lesser rank. By the induction hypothesis, the rank of the matrix W is lower bounded: $\mathrm{rank}(W) \geqslant (n-2)/2$. Then $\mathrm{rank}(\widetilde{N}) = \mathrm{rank}(W) + 1 \geqslant n/2$. Finally, $\mathrm{rank}(M) \geqslant \mathrm{rank}(N) \geqslant \mathrm{rank}(\widetilde{N}) \geqslant n/2$. Lemma 1 is proved.

LEMMA 2. Let an $n \times n$ matrix M over a field K be given so that each of its elements on the principal diagonal is distinct from zero and from one, and each element not on the principal diagonal is equal either to zero or to one. If no $(0,1)$-point lies in the affine envelope of columns of the matrix M, then the rank of M is not less than a number $(n+1)/2$.

Proof. Applying transformations $x_k \to 1 - x_k$ to the rows of the matrix, as in the proof of Theorem 1, we can pass from matrix M to matrix $\hat{M}$ of the same type, but in the last column of $\hat{M}$ all elements except one on the principal diagonal are zeros. We have a matrix

$$\hat{M} = \left(\begin{array}{ccc|c} & & & 0 \\ & N & & \vdots \\ & & & 0 \\ \hline * & \cdots & * & c \end{array}\right)$$

for some $c \notin \{0,1\}$. Since the affine envelope of columns in M does not contain any $(0,1)$-point, the same will be true for $\hat{M}$. In particular, the affine envelope of columns of the matrix does not contain the origin of coordinates. Therefore, $\mathrm{rank}(M) = \mathrm{rank}(\hat{M}) = \mathrm{rank}(N) + 1$. By Lemma 1, $\mathrm{rank}(N) \geqslant (n-1)/2$. Consequently, $\mathrm{rank}(M) \geqslant (n+1)/2$. Lemma 2 is proved.

LEMMA 3. Let a system of m linearly independent linear equations in n variables over a field K be given. If this system does not have a $(0,1)$-solution and the inequality $n < 2m - 1$ holds, then there exists a variable such that the system obtained by eliminating that variable does not have a $(0, 1)$-solution either.

Proof. Suppose that the system of linear equations does not have a $(0, 1)$-solution, but elimination of any variable leads to a system that has a $(0, 1)$-solution. Then, for any index j, the initial system has a solution in which only the value of the jth variable does not belong to $\{0, 1\}$, whereas the values of other variables belong to $\{0, 1\}$. We identify such a solution with the jth column in some $n \times n$ matrix. The rank of this matrix is not higher than an expression $n - m + 1$, no element on the principal diagonal belongs to $\{0, 1\}$, while all elements not on the principal diagonal belong to $\{0, 1\}$. According to Lemma 2, this is impossible if $n < 2m - 1$. Contradiction. Lemma 3 is proved.

2. RESULTS

THEOREM 1. Let a system of m linear equations of special form $y_j = \ell_j(x_1, \ldots, x_n)$ in $m + n$ variables $y_1, \ldots, y_m$, $x_1, \ldots, x_n$ be given, with ℓ_j denoting linear functions over some field. If this system does not have a $(0, 1)$-solution and the inequality $m > 2n + 2$ holds, then the system contains an equation such that the subsystem obtained by deleting that equation does not have a $(0, 1)$-solution either.

Proof. Deleting the jth equation is equivalent to eliminating the variable y_j. On the other hand, the system in question consists of linearly independent equations and defines an affine subspace of dimension n. Elimination of any variable leads to a new system containing $m - 1$ or m linearly independent equations. But if we eliminate the variable x_i we may need to replace the initial equations by their linear combinations. In view of Lemma 3, subject to the condition $n + m - r < 2(m - r) - 1$, we can delete at least r such variables while preserving the absence of a $(0, 1)$-solution. This condition is equivalent to the inequality $r < m - n - 1$. However, if $n < r$, then we may eliminate some variable y_j. For $m > 2n + 2$, therefore, from the initial system we may eliminate a variable y_j and, consequently, delete the jth equation. The theorem is proved.

THEOREM 2. Let a propositional CNF $\varphi(p_1, \ldots, p_n)$ with m elementary disjunctions in n variables be given. If φ does not belong to α-or-β-in-SAT and the condition $m > 2n+2$ is met, then there exists a CNF which does not belong to α-or-β-in-SAT and is obtained from φ by eliminating some elementary disjunction.

Proof. Using induction, we define a function f associating an elementary disjunction with a pseudo-Boolean linear function over the field of rationals. Constants are associated with numbers: $f(\bot) = 0$ and $f(\top) = 1$. A propositional variable p_i is assigned a variable $f(p_i) = x_i$. Negation $\neg p_i$ is assigned an expression $f(\neg p_i) = 1 - x_i$. Next, with the jth elementary disjunction $\varphi_j = \ell_1 \vee \cdots \vee \ell_k$ we associate an expression $f(\ell_1) + \cdots + f(\ell_k) - \alpha - (\beta - \alpha) y_j$, where a new variable y_j occurs only once. Then, a conjunction of elementary disjunctions φ_j is assigned a system of linear equations $f(\varphi_j) = 0$ for all indices $1 \leqslant j \leqslant m$. This system depends on $m + n$ variables. All the m equations are linearly independent since each depends on its auxiliary variable. We use the fact that $\alpha \neq \beta$ holds, and hence the equation obtained nontrivially depends on the variable y_j.

Every $(0,1)$-solution for this system corresponds to a $(\bot, \top)$-valuation of propositional variables under which in every elementary disjunction either exactly α or exactly β literals are true. And conversely, for such a $(\bot, \top)$-valuation of propositional variables, there exists a $(0,1)$-solution for the given system of equations. If $p_i = \bot$ then $x_i = 0$. If $p_i = \top$ then $x_i = 1$. If in the jth elementary disjunction exactly α literals are satisfied, then $y_j = 0$. And if exactly β literals are satisfied, then $y_j = 1$.

According to Theorem 1, if the system in question has no $(0,1)$-solution, then this property is preserved after deleting some equation, which matches the deletion of some elementary disjunction from CNF φ. The theorem is proved.

3. DISCUSSION

The bound obtained on the number of elementary disjunctions of an unsatisfiable subformula in 2-CNF is close to optimal. There exists an unsatisfiable 2-CNF with $m = 2n$ elementary disjunctions in n variables for which a subformula obtained by deleting any elementary disjunction is satisfiable. An example is the 2-CNF

$$(\neg p_1 \vee p_2) \wedge (p_1 \vee \neg p_2) \wedge \cdots \wedge (\neg p_{n-1} \vee p_n) \wedge (p_{n-1} \vee \neg p_n) \wedge (p_n \vee p_1) \wedge (\neg p_n \vee \neg p_1),$$

where each variable has two positive occurrences and two negative ones. This 2-CNF is equivalent to a conjunction of formulas expressing the equivalence of variables p_j and p_{j+1} for $j < n$, and also the equivalence of a variable p_n and the negation of a variable p_1. Therefore, it is unsatisfiable. But deleting from the 2-CNF in question one elementary disjunction corresponds to replacing some equivalence by an implication. The formula obtained is satisfiable for some $(\bot, \top)$-valuation under which the antecedent of the implication is false.

On the other hand, the bound for a decrease in the number of elementary disjunctions belongs in a domain where almost any 2-CNF is unsatisfiable [4, 5]. This is natural: the possibility of deleting some elementary disjunctions from an unsatisfiable 2-CHF does not impose unexpected extra restrictions on an unsatisfiable subformula. Also the results obtained for other classes of formulas give an upper bound on a phase transition threshold, if it exists.

The generalization to conjunctions of formulas of another form is also possible. Denote by $\mathrm{maj}(p_1, p_2, p_3)$ the majority function, whose value is equal to the most frequently encountered among $(\bot, \top)$-valuations of propositional variables p_1, p_2, and p_3. For literals ℓ_{ij}, the conjunction $\bigwedge_j \mathrm{maj}(\ell_{1j}, \ell_{2j}, \ell_{3j})$ is satisfiable iff the 3-CNF $\bigwedge_j (\ell_{1j} \vee \ell_{2j} \vee \ell_{3j})$ belongs to the set 2-or-3-in-SAT. Therefore, Theorem 2 applies to formulas of this form.

By analogy with the proof of Theorem 2, Theorem 1 allows us to impose different restrictions on different elementary disjunctions within CNF. For example, we can consider conjunctions $\varphi \wedge \psi$

of two CHFs such that, for some $(\bot, \top)$-valuation, in each elementary disjunction one number of literals is true in φ, and another number of literals is true in ψ.

A decrease of the length of a formula leads to a reduction of some estimates of computational complexity, as shown in [2, 3]. However, this does not guarantee a reduction of the execution time of some algorithms. Thus, applying the resolution method for verifying satisfiability of CNFs, sometimes at intermediate steps it is possible to obtain those elementary disjunctions that previously have been removed in passing from the initial CNF to a subformula of smaller length. On the other hand, the main result is the pure existence theorem which does not give a fast algorithm for searching an unsatisfiable subformula. This agrees with a guess about high computational complexity of the satisfiability problem in the worst case, expressed by many authors.

Acknowledgments. I am grateful to participants of the Conference "Mal'tsev readings" (Novosibirsk) for discussions of the paper.

REFERENCES

1. W. Li, C. Xu, Y. Yang, J. Chen, and J. Wang, "A refined branching algorithm for the maximum satisfiability problem," *Algorithmica,* **84**, 982-1006 (2022); https://doi.org/10.1007/s00453-022-00938-8

2. J. Peng and M. Xiao, "Further improvements for SAT in terms of formula length," *Informat. Comput.*, **294**, 105085 (2023); https://doi.org/10.1016/j.ic.2023.105085

3. S. Szeider, "Minimal unsatisfiable formulas with bounded clause-variable difference are fixed-parameter tractable," *J. Comp. System Sci.*, **69**, No. 4, 656-674 (2004); https://doi.org/10.1016/j.jcss.2004.04.009

4. A. Goerdt, "A threshold for unsatisfiability," *J. Comp. System Sci.*, **53**, No. 3, 469-486 (1996); https://doi.org/10.1006/jcss.1996.0081

5. D. Achlioptas, A. Coja-Oghlan, M. Hahn-Klimroth, J. Lee, N. Müller, M. Penschuck, and G. Zhou, "The number of satisfying assignments of random 2-SAT formulas," *Random Structures Algorithms*, **58**, No. 4, 609-647 (2021); https://doi.org/10.1002/rsa.20993

6. J. Giráldez-Cruand and J. Levy, "Popularity-similarity random SAT formulas," *Artificial Intelligence*, **299**, 103537 (2021); https://doi.org/10.1016/j.artint.2021.103537

7. J. Ding, A. Sly, and N. Sun, "Satisfiability threshold for random regular NAE-SAT," *Comm Math. Phys.*, **341**, 435-489 (2016); https://doi.org/10.1007/s00220-015-2492-8

8. G. Nie, D. Xu, X. Wang, and X. Wang, "The phase transition analysis for the random regular exact 2-(d, k)-SAT problem," *Symmetry*, **13**, No. 7, 1231 (2021); https://doi.org/10.3390/sym13071231

9. A. A. Boykov and A. V. Seliverstov, "On a cube and subspace projections," *Vest. Udmurt Univ. Mat. Mekh. Copm. Sci.* **33**, No. 3, 402-415 (2023); https://doi.org/10.35634/vm230302

10. N. T. Kogabaev, "Systems of Diophantine equations over finite configurations," *Sib. Math. J.*, **64**, No. 2, 325-337 (2023).

11. M. N. Vyalyi, "Testing the satisfiability of algebraic formulas over the field of two elements," *Probl. Information Transmiss.*, **59**, No. 1, 57-62 (2023); `https://doi.org/10.1134/S0032946023010052`

12. A. Abboud, K. Bringmann, D. Hermelin, and D. Shabtay, "Scheduling lower bounds via AND subset sum," *J. Comp. System Sci.*, **127**, 29-40 (2022); `https://doi.org/10.1016/j.jcss.2022.01.005`