$$\chi'(0,\ \beta)=\chi(0,\ \mathrm{Tr}_{K/k}(\beta))\ \text{and}\ \chi'(\alpha,\ \beta)=\chi'(\alpha,\ 0)\chi'(0,\ \beta).$$

The following proposition is an analogue of the Davenport–Hasse theorem for Gauss sums (see [1, p. 248]).

Proposition 2. If $\chi\neq\chi_0\in\Gamma$, χ' is the lifting of χ to the field K, and $G(\chi')=\sum_{\alpha\in K}\chi'(\alpha,0)$, then $G(\chi') = (-1)^{n-1}G^n(\chi)$.

Proof. It is clear that $G(\chi') = L_n(\chi)$. But it was shown above that if $\chi \neq \chi_0$, then $L_n(\chi)=(-1)^{n-1}\omega^n(\chi)=(-1)^{n-1}G^n(\chi)$.

LITERATURE CITED

1. R. Lidl and H. Niederreiter, Finite Fields [Russian translation], Vol. 1, Mir, Moscow (1988).
2. S. Chowla, "A note on the construction of finite Galois fields GF(p^n)," J. Math. Anal. Appl., 15, 53-54 (1966).
3. R. Ree, "Proof of a conjecture of S. Chowla," J. Number Theory, 3, No. 2, 210-212 (1971).
4. S. D. Cohen, "Uniform distribution of polynomials over finite fields," J. London Math. Soc. Ser. 2, 6, No. 1, 93-102 (1972).
5. E. N. Kuz'min, "Irreducible polynomials over a finite field," Sib. Mat. Zh., 30, No. 6, 98-109 (1989).
6. L. Carlitz, "A theorem of Dickson on irreducible polynomials," Proc. Amer. Math. Soc., 3, No. 5, 693-700 (1952).
7. E. N. Kuz'min, "Irreducible polynomials over a finite field," in: International Conference on Algebra in Memory of A. I. Mal'tsev: Abstracts of Reports on the Theory of Rings, Algebras, and Modules, Institute of Mathematics, Siberian Branch, Academy of Sciences of the USSR, Novosibirsk (1989), p. 75.
8. E. N. Kuz'min, "On a class of irreducible polynomials over a finite field," Dokl. Akad. Nauk SSSR, 313, No. 3, 552-555 (1990).
9. G. L. Watson, "Sums of eight values of a cubic polynomial," J. London Math. Soc., 27, No. 2, 217-224 (1952).
10. D. R. Hayes, "The distribution of irreducibles in GF[q, x]," Trans. Amer. Math. Soc., 117, 101-127 (1965).

TEMPORAL LOGICS WITH "THE NEXT" OPERATOR DO NOT HAVE INTERPOLATION OR THE BETH PROPERTY*

L. L. Maksimova

UDC 510.64

Beth's definability theorem, first proved by Beth [1] in 1953, states that in the classical first-order predicate logic one can eliminate implicit definitions: If a certain predicate can be defined implicitly, it can also be defined explicitly, that is, by means of a formula of the language. Another result, closely related to Beth's theorem, is Craig's interpolation theorem [2]. In this paper we will show that the analogs of Beth's and Craig's theorems fail to hold in temporal logics, which are characterized by discrete temporal structures.

These logics are widely applied in the information sciences and the theories of data bases and knowledge bases [3-7].

By a temporal structure (or time scale) we mean any nonempty set T with a binary relation $\prec$. The elements of T are called temporal points or times, $x\prec y$ reads "x precedes y" or "y covers x." Let $\leqslant$ denote the reflexive and transitive closure of $\prec$. Thus, for any temporal points x and y:

$$x\leqslant y \Leftrightarrow (\exists x_1\ldots x_n)\,(x=x_1\&\ldots\&x_n=y\&x_1\prec x_2\prec\ldots\prec x_n).$$

We read $x\leqslant y$ as "y is accessible from x."

*In memory of Anatolii Illarionovich Shirshov.

Novosibirsk. Translated from Sibirskii Matematicheskii Zhurnal, Vol. 32, No. 6, pp. 109-113, November-December, 1991. Original article submitted June 20, 1990.

In these models one can define two temporal operators: o ("the next" or "tomorrow") and □ ("will always be the case") as follows:

$$x\vdash \bigcirc A \Leftrightarrow (\forall y \succ x)(y\vdash A),\quad x\vdash \Box A \Leftrightarrow (\forall y\geqslant x)(y\vdash A).$$

Using these temporal operators and the usual connectives of classical logic, one can define a language of temporal logic, in both propositional and predicate versions. The truth relation $x\vdash A$, for any x in T and any formula A in the language of temporal logic, is defined in the natural way. We call the logic thus obtained a discrete time logic, and denote it by LD. LD contains exactly those formulas that are true at any time in any temporal model.

Along with LD, we will also consider some extensions, in particular, a linear time logic. Thus, the logic LT_ω is characterized by a linear temporal structure, whose order type is that of the natural numbers. The logic LT_Z is characterized by a temporal structure whose order type is that of the integers; its language contains temporal operators both for the future and for the past.

In this paper we will prove that LD, LT_ω, LT_Z – and many of their extensions – do not have the Beth and Craig properties.

1. Beth and Interpolation Properties

Going over to temporal logics, one can formulate various analogs of Beth's theorem, depending on how the concepts of explicit and implicit definability are defined. We first introduce some definitions and notation.

We will consider a language of temporal logic containing the logic symbols ⊥ ("false") and →, quantifiers, and also the temporal operators o and □. The language may also contain the equality symbol (which in this case is treated as a logical symbol); predicate and function symbols, however, are usually nonlogical.

Recall that a temporal structure $\langle T, \prec\rangle$ is a nonempty set T with a binary relation $\prec$. If $\langle T, \prec\rangle$ is a temporal structure, we define a model to be a quadruple $M=\langle T, \prec, \{D_t\}_{t\in T}, \vdash\rangle$, where $\{D_t\}_{t\in T}$ is a family of nonempty object domains, $\vdash$ the truth relation, defined in the standard way for the classical connectives and quantifiers, $x\vdash \bigcirc A \Leftrightarrow (\forall y\succ x)(y\vdash A)$, $x\vdash \Box A \Leftrightarrow (\forall y\geqslant x)(y\vdash A)$.

If $t\in T$ and A is a formula without free object variables, then $t\vdash A$ is read as "A is true at time t." We write $M\vdash A$ ("A is true in M") if $(\forall t\in T)(t\vdash A)$. We shall say that M is a model of a logic L if all formulas that are valid in L are true in M. If Γ is a set of formulas, we write $\Gamma\vDash_L A$ if, for any model M of L, it follows from $(\forall B\in\Gamma)(M\vdash B)$ that $M\vdash A$.

We will say that a logic L has the Beth property B1 if, for any closed formula A(P, X), where P is a list of parameters, X an n-ary predicate variable and x a list of n object variables, it follows from $L\vdash A(P, X)\,\&\,A(P, Y)\to(\forall x)(X(x)\leftrightarrow Y(x))$ that there exists a formula B(P, x), all of whose parameters occur in P, x, such that $L\vdash A(P, X)\to(\forall x)(X(x)\leftrightarrow B(P, x))$.

We will say that L has the Beth property BP if it follows from $A(P,X),\ A(P, Y)\vDash_L(\forall x)(X(x)\leftrightarrow Y(x))$ that there exists a formula B(P, x), all of whose parameters occur in P, x, such that $A(P, X)\vDash_L(\forall x)(X(x)\leftrightarrow B(P, x))$.

The Beth properties mean that one can eliminate descriptive definitions in the logic: the fact that a certain description uniquely defines a predicate (up to equivalence) implies that the predicate can be defined constructively, using a logic term of the language. The difference between the two properties as formulated is that B1 is phrased syntactically, BP semantically.

The property known as interpolation is closely related to the Beth properties.

We say that a logic L has the Craig interpolation property if, for any formulas A and B such that $L\vdash A\to B$, there exists a formula C such that $L\vdash A\to C$ and $L\vdash C\to B$, where all predicate variables, function variables and free object variables of C occur both in A and in B.

It can be shown that the interpolation property implies the Beth property B1 (see [2]).

In order to prove that LD lacks the Beth and Craig properties, we consider the propositional formula

$$A(P, X)\leftrightharpoons\Box(\neg X\&\neg\Box P\to\neg\bigcirc\neg X)\&\Box(\neg\bigcirc\neg X\to\bigcirc X)\&\Box(\bigcirc X\to \\ \to\neg X\&\neg\Box P)\&\Box(X\to\neg\Box P)\&\Box\Diamond\Box P.$$

LEMMA 1. The temporal logic LD contains the formula $A(P, X) \& A(P, Y) \to (X \leftrightarrow Y)$, that is, the formula A(P, X) implicitly defines X in LD.

Proof. Suppose the contrary. In other words, there exist a model $\langle T, \prec \rangle$ and an instant t in T such that $t \vdash A(P, X) \& A(P, Y)$, $t \vdash X \& \neg Y$. Since $t \vdash \Diamond \Box P$, there exists $v \geqslant t$ for which $v \vdash \Box P$. By definition, there exist, $x_1, \ldots, x_n$ such that $t = x_1$, $v = x_n$ and $x_1 \prec \ldots \prec x_n$. Since $t \vdash X \& (X \to \neg \Box P)$, it follows that $x_1 \vdash \neg \Box P$, i.e., $v \neq x_1$. Next, from $t \vdash A(P, Y) \& \neg Y$ we obtain $x_1 \vdash \neg \bigcirc \neg Y$ and $x_1 \vdash \bigcirc Y$, and so $x_2 \vdash Y$. Therefore $x_2 \vdash \neg \Box P$ and $v \neq x_2$. In addition, $x_1 \vdash \neg \bigcirc X$, $x_1 \vdash \bigcirc \neg X$, that is, $x_2 \vdash \neg X$. Continuing the reasoning, we obtain $x_{2k+1} \vdash X \& \neg Y \& \neg \Box P$, $x_{2k} \vdash \neg X \& Y \& \neg \Box P$ for all k. Hence $x_n \vdash \neg \Box P$, contrary to the equality $x_n = v$. ∎

To prove that our logic does not ensure explicit definability, we consider some extensions of LD.

2. Linear-Time Logic

The most familiar extension of LD is LT_ω, whose temporal structures are ordered according to the type of the natural numbers. This logic was examined in [8-10]. The standard model of LT_ω is $\langle \omega, \prec, \{D_t\}_{t \in T}, \vdash \rangle$, where $\prec$ is the "successor" relation on the set of natural numbers ω, i.e., $x \prec y \Leftrightarrow x + 1 = y$. We will also consider an extension of this logic characterized by what are known as stable models.

A model $\langle T, \prec, \{D_t\}_{t \in T}, \vdash \rangle$ is said to be stable if, for any closed formula A and any chain $x_1 \prec x_2 \prec x_3 \prec \ldots$, there exists n such that for all $y \geqslant x_n$ we have $x_n \vdash A \Leftrightarrow y \vdash A$.

Let $LT_\omega S$ denote the set of formulas that are true in all stable models $\langle \omega, \prec, \vdash \rangle$. $LT_\omega S$ is a proper extension of LT_ω, since it contains the formula $\Box \Diamond X \to \Diamond \Box X$, which is not in LT_ω.

An axiomatization of the propositional logics LT_ω and $LT_\omega S$ may be found in [8]; for an axiomatization of the predicate logic LT_ω we refer the reader to [9, 10].

THEOREM 1. Let L be any logic intermediate between LD and $LT_\omega S$. Then L does not have the Beth properties B1 or BP, or the Craig interpolation property.

Proof. By Lemma 1, we have $L \vdash A(P, X) \& A(P, Y) \to (X \leftrightarrow Y)$, so $A(P, X), A(P, Y) \vDash_L (X \leftrightarrow Y)$. We claim that there is no formula B(P) such that $A(P, X) \vDash_L (X \leftrightarrow B(P))$. To that end, we consider a structure $\langle Z, \prec \rangle$, where Z is the set of integers, $x \prec y \Leftrightarrow x + 1 = y$. We will need the following easily proved

LEMMA 2. Any model $M = \langle Z, \prec, \{D_t\}_{t \in Z}, \vdash \rangle$ based on $\langle Z, \prec \rangle$ is a model of LT_ω. If M is stable, then M is a model of $LT_\omega S$.

Proof. It follows from the definition of truth for formulas in the language of LT_ω that if a formula F is refuted at a time $t \in Z$ of M, then it is refuted in the model M' obtained by restricting M to the set $\{z \in Z | z \geqslant t\}$. Clearly, M' is isomorphic to a suitable model $\langle \omega, \prec, \{D_t\}_{t \in \omega}, \vdash \rangle$. Therefore F is not in LT_ω. If M is stable, then M' is also stable. □

Consider the following model $M = \langle Z, \prec, \{D_t\}_{t \in Z}, \vdash \rangle$:

$D_t = \{0\}$ for all $t \in Z$, $t \vdash P \Leftrightarrow t = 0$, $t \vdash X \Leftrightarrow (t \leqslant 0 \,\&\, t$ is even).

It is readily shown by induction on the structure of formulas that the stability condition holds for any formula C(P, X) in the language of LT_ω. We have thus proved

LEMMA 3. M is a stable model.

Now, for any formula B, we define the set $LS(B) = \{t \in Z | (\forall z \leqslant t)(z \vdash B \Leftrightarrow t \vdash B)\}$. We will say that B is left stable in M if the set LS(B) is not empty. Note that $t \in LS(B) \& z \leqslant t \Rightarrow z \in LS(B)$.

LEMMA 4. Any formula B(P) is left stable in M.

Proof is by induction on structure of B(P). The formula B(P) contains no free object variables or function symbols and is built up from atomic formulas ⊥, P, u = v by means of connectives →, □, ○ and quantifiers. By definition, LS(⊥) = Z, LS(P) = {t|t < 0)}; LS(u = v) = Z, since each D_t is a singleton. Further, $LS(B_1 \to B_2) = LS(B_1) \cap LS(B_2)$; $LS(\bigcirc B_1) \supseteq \{t | (t+1) \in LS(B_1)\}$; $LS(\Box B_1) = Z$ if $M \vdash B_1$ and $LS(\Box B_1) = \cup \{z \leqslant t |$ it is false that $t \vdash B_1\}$ if it is false that $M \vdash B_1$. Since all the object domains D_t are singletons, it follows that for any formula $\forall x B_1(P)$ we have $M \vDash \forall x B_1(P) \leftrightarrow B_1(P)$ and $LS(\forall x B_1(P)) = LS(B_1(P))$. □

We can now complete the proof of the theorem. Suppose on the contrary that there exists a formula B(P) in the language of LT_ω such that

$$A(P, X) \vDash_L X \leftrightarrow B(P). \tag{1}$$

It is easy to see that $M \vdash A(P, X)$. On the other hand, by Lemma 4, N(P) is left stable. If $t \in LS(B(P))$ and t < 0, then it is either false that $t \vdash X \leftrightarrow B(P)$ or false that $(t-1) \vdash X \leftrightarrow$ B(P). Contradiction. Thus, (1) cannot be valid for any formula B(P).

It also follows from what we have proved that $L \vdash A(P, X) \rightarrow (X \leftrightarrow B(P))$ cannot be valid for any formula B(P). Thus, L has neither property B1 nor property BP. As a corollary, L does not have the Craig interpolation property. Q.E.D.

Note that Theorem 1 contradicts [9, Sec. 3], where it is stated that LT_ω possesses the interpolation property and the Beth property B1.

Remark. It is obvious from our results that the propositional fragment of L also lacks the Beth properties.

Some authors have considered LT_ω with additional temporal operators, such as a binary operator "until" [6, 11, 5]. The latter can be defined in various ways. For example, the definition in [11] is

$$x \vdash A\mathrm{U}B \Leftrightarrow [(\forall y \geqslant x)(y \vdash A) \quad \text{or} \\ (\exists y > x)(y \vdash B \,\&\, \forall z(x \leqslant z < y \Rightarrow z \vdash A))]. \tag{2}$$

Another definition of U may be found in [12]:

$$x \vdash A\mathrm{U}B \Leftrightarrow (\exists y > x)[y \vdash B \,\&\, \forall z(x < z < y \Rightarrow z \vdash A)]. \tag{3}$$

Definitions (2) and (3) are not equivalent. Nevertheless, in both cases the model M considered in the proof of Theorem 1 is still stable. In addition, $LS(A\mathrm{U}B) \supseteq \{z-1 \mid z \in LS(A) \cap$ LS(B)}, and therefore Lemmas 3 and 4 – and hence also Theorem 1 – remain valid for these enriched temporal logics.

3. Logics with Past Tense Operators

Our counterexample to Beth's property in LT_ω is easily extended to logics with past tense operators. Let us consider LT_Z, whose languge includes, besides ○ and □, operators ⊖ ("yesterday") and ⊟ ("always was the case"). The natural definition of these operators in temporal models is as follows:

$$x \vdash \ominus A \Leftrightarrow (\forall y \prec x)(y \vdash A), \quad x \vdash \boxminus A \Leftrightarrow (\forall y \leqslant x)(y \vdash A).$$

The standard models of LT_Z are $\langle Z, \prec, \{D_t\}_{t\in Z}, \vdash\rangle$, where $x \prec y \Leftrightarrow y = x+1$. Thus, LT_Z is the set of formulas of the extended language that are true in all standard models. We let LT_ZS denote the set of formulas that are true in all stable models $\langle Z, \prec, \{D_t\}_{t\in Z}, \vdash\rangle$.

The logic LT_Z was considered, inter alia, in [4]. The author of [12] also considered an additional temporal operator "since," dual to "until":

$$x \vdash A\,\mathrm{Since}\,B \Leftrightarrow (\exists y < x)(y \vdash B \,\&\, \forall z(y < z < x \Rightarrow z \vdash A)).$$

THEOREM 2. Let L be any logic intermediate between LT_Z and LT_ZS. Then L has neither the interpolation property nor the Beth properties.

The proof is practically the same as that of Theorem 1. Lemma 3 remains valid upon passage to the enriched language. In proving Lemma 4 it is enough to assume fulfillment of the conditions $LS(\ominus A) = LS(A)$, $LS(\boxminus A) = LS(A)$.

Remark. The author of [3] considered a temporal logic KTL_1 with operators U_{ijk}, S_{ijk}, which are generalizations of "until" and "since." In the model Z these operators are defined as follows:

$$x \vdash A\mathrm{U}_{ijk}B \Leftrightarrow (\exists y > x)[(y-x) \text{ is divisible by } k \,\&\, y \vdash B \,\& \\ \&\, \forall z(x+i < z < y \,\&\, ((z-x-i) \text{ is divisible by } j) \Rightarrow z \vdash A)],$$
$$x \vdash A\mathrm{S}_{ijk}B \Leftrightarrow (\exists y < x)[(x-y) \text{ is divisible by } k \,\&\, y \vdash B \,\& \\ \&\, \forall z(x-i > z > y \,\&\, ((x-i-z) \text{ is divisible by } j) \Rightarrow z \vdash A)].$$

In this language the formula A(P, X) explicitly defines X; the following formula is valid in KRL_1:

$$A(P, X) \rightarrow (X \leftrightarrow ((\top U_{012}(\neg \Box P \,\&\, \neg \bigcirc \neg \Box P)) \vee (\neg \Box P \,\&\, \neg \bigcirc \neg \Box P))).$$

LITERATURE CITED

1. W. E. Beth, "On Padoa's method in the theory of definitions," Indag. Math., 15, No. 4, 330-339 (1953).
2. W. Craig, "Three uses of the Herbrand–Gentzen theorem in relating model theory and proof theory," J. Symbol. Logic, 22, 269-285 (1957).
3. M. K. Valiev, "On temporal dependences in databases," Izv. Akad. Nauk SSSR, Ser. Tekhn. Kibern., 1, 106-115 (1985).
4. E. Chouraki, "Formal expression of time in a knowledge base," in: Non-standard Logics for Automated Reasoning, Academic Press, London (1988), pp. 81-98.
5. F. Kroeger, "Temporal logics of programs," in: EATS Monograph on Theoretical Computer Science, Springer, Berlin (1987).
6. Z. Manna and A. Pnuelli, "Verification of concurrent programs: a temporal proof system," in: Foundations of Computer Science IV (Math. Centre Tracts), Amsterdam (1983), pp. 163-255.
7. I. Nemeti, "Nonstandard dynamic logic," in: D. Kozen (ed.), Logic of Programs: Proc. Conf. New York, 1981, Lecture Notes in Computer Science, 131, Springer, Berlin (1982), pp. 311-348.
8. K. Segerberg, "Von Wright's temporal logic," in: Deduction [Russian translation], Nauka, Moscow (1979), pp. 173-205.
9. H. Kawai, "Eine Logik erster Stufe mit einem infinitaren Zeitoperator," Z. Math. Log. Grundl. Math., 28, 173-180 (1982).
10. H. Kawai, "Sequential calculus for a first order infinitary temporal logic," Z. Math. Log. Grundl. Math., 33, 423-432 (1987).
11. Z. Manna and P. Wolper, "Synthesis of communicating processes from temporal logic specifications," in: D. Kozen (ed.), Logic of Programs: Proc. Conf. New York, 1981, Lecture Notes in Computer Science, 131, Springer, Berlin (1982), pp. 253-281.
12. H. W. Kamp, Tense Logic and the Theory of Linear Order, Ph. D. Thesis, University of California, Los Angeles (1968).

SANDWICHES IN LIE ALGEBRAS*

Yu. A. Medvedev

UDC 512.554.322

In 1958 Kostrikin [1-3] found a positive solution to the weakened Burnside problem for a prime exponent p. Thirty years later, Zel'manov [4] positively solved the weakened Burnside problem for an arbitrary primal exponent p^k. In their approaches both A. I. Kostrikin and E. I. Zel'manov at first used the reduction of the weakened Burnside problem to a problem of local nilpotency of a Lie algebra with an Engelian condition. The problem of local nilpotency of an Engelian Lie algebra was solved with the help of sandwiches.

An element a of an arbitrary Lie algebra L is called a sandwich if $[a, x, a] = 0$ for any $x \in L$. In other manifolds of algebras the elements with the properties of sandwiches are still called absolute divisors of zero. The name "sandwich" has been fixed in Lie algebras, in the first place owing to the fundamental papers of A. I. Kostrikin on the weakened Burnside problem. In this article the ideas and methods of A. I. Kostrikin will be essentially used. Therefore, we will use just the name "sandwich" for elements with the indicated property.

An element a of a Lie algebra L generates an abelian ideal only in the case when $[a, x_0, x_1, \ldots, x_k, a] = 0$ for any $x_i \in L$ and any k. As usual, by $[a_1, a_2, \ldots, a_n]$ let us understand the commutator $[[\ldots[[a_1, a_2], a_3], \ldots,], a_n]$. The concept thus arises of the "thickness" of a sandwich or the order of the absolute divisor of zero.

*Dedicated to the memory of A. I. Shirshov – one of my first outstanding guides on the path to algebra.

Novosibirsk. Translated from Sibirskii Matematicheskii Zhurnal, Vol. 32, No. 6, pp. 114-127, November-December, 1991. Original article submitted March 13, 1991.