El Problema dels generals bizantins

El *Problema dels generals bizantins* il·lustra una situació que apareix sovint en la informàtica d'avui: es té una idea que podria resoldre un problema concret, però no s'està completament segur de si el mètode funciona també en altres casos. Dos exemples suggereixen que els llenguatges naturals no són adequats per a les reflexions lògiques i que, per tant, s'han de desenvolupar els llenguatges artificials. A continuació s'exposen les idees de l'autor sobre les aplicacions d'aquests llenguatges formals a d'altres ciències, a part de la informàtica.

CLEMENS H. CAP

Quatre generals, que anomenarem Alfa, Beta, Gamma i Delta, setgen Bizanci amb el seu exèrcit. La situació de la guerra és tal que només l'atac conjunt de com a mínim tres exèrcits pot ser victoriós. Com que una reunió enmig de la guerra no és possible, els quatre generals s'han de posar en contacte per mitjà d'un missatger per a decidir si ataquen o bé es retiren de Bizanci sense lluitar. Si només dos generals, o bé només un, comencen sols la batalla, aquesta acabarà en una gran derrota. Aquesta decisió es veu agreujada pel fet que entre els quatre generals hi ha un traïdor, la identitat del qual els tres generals lleials desconeixen. Els generals comencen amb un intercanvi de missatges en els quals exposen la seva opinió. El traïdor també envia el seu missatger, però actua incorrectament: li comunica a un general que està a favor de l'atac i, per contra, a un altre que afavoreix la retirada. Aquests volen, naturalment, desemmascarar el traïdor i per tant seguidament es demanen l'un a l'altre què havia dit, doncs, el col·lega. Així demana, diguem, el general Alfa als col·legues Beta i Gamma quina opinió havia expressat Delta. Beta contesta que Delta estava a favor de l'atac, mentre que Gamma diu que Delta afavoria la retirada. Podran els tres generals lleials, davant d'una situació tan confusa, arribar a una decisió conjunta única? Es considera que un traïdor de vegades, per tal de camuflar-se, actua de manera totalment correcta.

Una solució dels problemes bizantins

Una solució òbvia seria que un general nomenés un recomptador de vots. Cada oficial li enviaria el seu vot sobre atac o retirada i subseqüentment comunicaria als altres la decisió obtinguda. Lamentablement, no es pot garantir que el recomptador de vots no sigui el traïdor. Per tant, els generals han de procedir de la manera següent: En una primera volta, cada general ha de comunicar als altres la seva pròpia opinió. En una segona volta es comunica la informació rebuda en la primera volta. Cada general disposa ara de tres informacions relatives a cadascun dels altres tres generals: una que prové del general mateix i dues que provenen dels seus col·legues. Ara obté, a partir d'aquestes tres declaracions, una decisió majoritària: atac o retirada. Així, cada general pot determinar per ell mateix la decisió majoritària corresponent a cadascun dels seus col·legues. A continuació, a partir d'aquestes tres informacions i de la seva pròpia opinió obté de nou una decisió majoritària. En cas d'igualtat de vots es decideix per la retirada.

Els generals bizantins i la informàtica

Experimenteu una miqueta i us convencereu que els tres generals lleials arriben, de fet, a la mateixa conclusió. És possible una solució semblant en el cas de dos traïdors i sis lleials, o bé són necessaris en aquest cas més generals lleials? Es poden adoptar els mateixos mètodes, o bé se n'han de desenvolupar de nous a partir d'una discusió més general?

Per què s'interessa la informàtica en questions d'aquesta mena? Els ordinadors s'utilitzen en

moltes situacions de la nostra vida i l'experiència ha demostrat que aquests només són fiables fins a un cert grau. És així, els errors de programació, però també les descàrregues electroestàtiques, la radiació ionitzant i els defectes de material poden conduir a una computació defectuosa. L'ordinador pot fins i tot ser afectat de tal manera que canviï els senyals lluminosos del tren en el qual vostè està viatjant i llegint aquest article. Però no cal preocupar-se! Substitueixi els generals de la nostra anècdota per l'ordinador. El traïdor pren aleshores el significat d'un ordinador defectuós. Recordi que fins i tot amb la presència d'un traïdor, la resta dels generals arriben a una decisió idèntica. Si vostè té també quatre ordinadors a la seva disposició per a fer una feina delicada, també li'n pot fallar un sense que això arribi a portar cap problema especial.

A causa de les seves especials necessitats, ja s'apliquen des de fa anys aquest i d'altres trucs semblants en el camp de l'astronàutica per tal d'incrementar la fiabilitat dels sistemes de computació. En l'aviació civil, i en altres àrees on s'utilitzen els ordinadors d'una manera crucial, ja s'hi estan introduint. El problema dels generals bizantins no té, però, importància només per ell mateix. Les preguntes que ens hem fet en connexió amb la solució que hem proposat són característiques d'una situació que es dóna sovint en el camp de la informàtica: tenim una idea de com s'ha d'actuar davant d'un problema concret, però no estem completament segurs de si els nostres mètodes funcionen també en altres casos.

Per què necessita la matemàtica llenguatges artificials?

Els problemes del nostre llenguatge són coneguts: Des d'Aristòtil (384-322 aC) és coneguda l'antinòmia del mentider continguda en la sentència «Aquesta sentència és falsa». Es miri com es vulgui, quan aquesta sentència és vertadera és falsa i, quan és falsa, aleshores és vertadera. Les antinòmies ens mostren que en català, i també en totes les altres llengües naturals, es poden generar embolics deguts a una confusió entre el nivell de l'objecte descrit i el nivell del llenguatge que descriu l'objecte. Les antinòmies ens ensenyen una sana desconfiança envers les reflexions fetes en els llenguatges naturals i ens indueixen a desenvolupar els llenguatges artificials, amb els quals les antinòmies i les ambigüitats esdevenen impossibles.

Un llenguatge artificial consisteix en un conjunt finit de símbols i en un nombre finit de regles, les quals determinen quins arranjaments de símbols es consideren, de fet, paraules del llenguatge. Així, el llenguatge de l'aritmètica consisteix en els numerals, els símbols d'operacions $+ - \times /$, els parèntesis (i), com també el símbol d'identitat $=$. Les regles d'aquest llenguatge fan que els arranjaments 2 o bé 2+3, o bé 3+4=7 siguin considerats paraules del llenguatge i, en canvi, no ho sigui l'arranjament $2++\times$. 3+4=5 és una paraula del llenguatge de l'aritmètica, encara que fins aquest moment no hem fet cap declaració sobre si representa un fet correcte o incorrecte ni sobre com aquesta paraula s'hauria d'interpretar.

L'antinòmia de Richardson

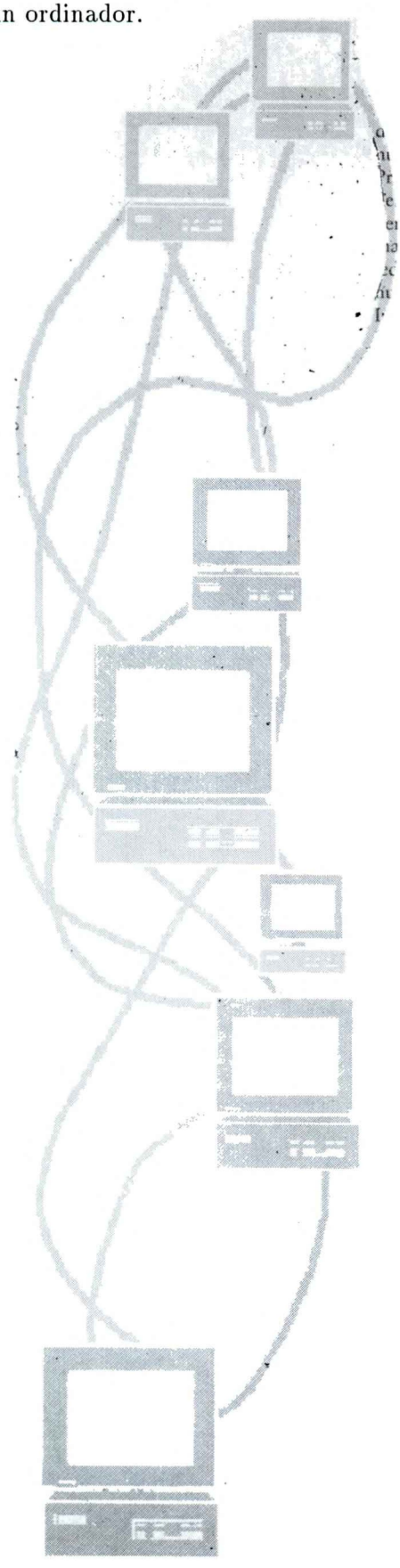
En català podem descriure els nombres naturals per mitjà d'un text. Així, el text «El nombre que és la suma de tres i quatre» descriu el nombre set. Per a aquesta definició hem necessitat 32 lletres. Ara volem escriure en un full de paper tots i cadascun dels nombres naturals que poden ser descrits per mitjà d'una sentència de la llengua catalana de menys de cinc-centes lletres. Aquests són, per descomptat, molts nombres. Però només es poden donar un nombre finit de sentències catalanes amb menys de cinc-centes lletres, les quals descriuen, per tant, només un nombre finit de nombres naturals. Volem ara considerar el nombre natural més petit que no es troba escrit al full de paper. Aquest és «El nombre natural més petit que no pot ser descrit amb una sentència de la llengua catalana de menys de cinc-centes lletres». Però, no és aquesta darrera sentència una tal sentència descriptiva de menys de 500 lletres?

Sobre el significat dels llenguatges artificials

Fins ara hem considerat només la *Sintaxi* dels llenguatges artificials. Ara volem estudiar la seva *Semàntica*, i també el seu significat. Per a això, assignem a cada paraula del nostre llenguatge un objecte d'un model. Aquest model pot consistir en construccions del pensament i en abstraccions, i també en idees platòniques. Pot també consistir en els mesuraments d'un físic fets en un laboratori, en el contingut d'un programa d'ordinador, o també en objectes matemàtics. En el nostre llenguatge aritmètic volem assignar a la paraula 2 el nombre i també el pensament abstracte *dos*. A una paraula de la forma $A + B$, li volem assignar la suma dels valors que hem assignat a A i a B. A la paraula 3+4=7 li assignem el concepte *vertader* i a la paraula 3+4=5 el concepte *fals*. Naturalment, podriem també haver assignat a la paraula 2 un altre nombre, per exemple *dotze*, però les convencions usuals sobre el significat dels nombres en la cultura occidental ens han induït a la decisió esmentada anteriorment.

Sobre el funcionament dels mètodes formals

En el llenguatge artificial utilitzat en el nostre exemple podem, en particular, trobar sentències sobre fets aritmètics. Així, per exemple, a la paraula 3+4=7, li assignàvem el concepte *vertader*, i volem interpretar-la com una descripció d'un fet aritmètic. També a la paraula 1+2=3, li correspòn el valor de veritat *vertader*. A partir d'aquestes dues paraules vertaderes podem construir la paraula vertadera 1+2+4=7. Evidentment, seguint la regla següent: si tenim dues paraules de la forma A+B=C i D+E=A, en les quals les lletres A, B, C, D i E representen nombres, que tenen el valor de veritat *vertader*, aleshores també té aquest valor de veritat la paraula D+E+B=C. Així, sense calcular i sense pensar sobre els objectes concrets del nostre model, podem arribar a noves sentències vertaderes només reordenant les tires de lletres d'acord amb les regles. La investigació rigorosa d'aquests sistemes de regles és tasca de la lògica. La lògica de l'aritmètica consisteix en un nombre petit de regles, semblants a les del nostre exemple, que ens permeten derivar molts d'altres fets aritmètics per mitjà d'una pura manipulació de text i de símbols. Aquesta manipulació es pot esquematitzar i pot ser efectuada per un ordinador.



Diferents lògiques

La idea que es poden obtenir noves veritats a partir d'una reordenació de símbols seguint unes regles de joc prèviament donades té quelcom de fascinant. L'exemple que hem utilitzat anteriorment és realment molt simple i fa que el llenguatge tècnic dels matemàtics resulti una mica presumptuós per a parlar de fets trivials. Aquest, però, és necessari en situacions més complexes. En això precisament consisteix sovint el treball d'un matemàtic: a partir d'unes poques propietats d'un objecte arribar a nous coneixements per mitjà de la manipulació dels símbols d'un llenguatge artificial. Amb l'aplicació estricta d'aquest mètode lògic no és necessari conèixer el significat del llenguatge. Només es tracta d'aplicar les regles adequades en la successió correcta. En la pràctica, però, una idea intuïtiva és molt útil, tant per a l'elecció de les regles com per a la interpretació del resultat.

Lògica de programes, la qual demostra la correcció d'un programa de divisió

$\{0 \leq x \text{ and } 0 < y\}$
$r : 0x; q := 0;$
$\{0 \leq r \text{ and } 0 < y \text{ and } x = y * q + r\}$
while $r \geq y$ do
begin $\{0 \leq r \text{ and } 0 < y \leq r \text{ and } x = y * q + r\}$
$r := r - y; q := q + 1$
$\{0 \leq r \text{ and } 0 < y \text{ and } x = y * q + r\}$
end
$\{0 \leq r < y \text{ and } x = y * q + r\}$ —

Un físic teòric va a la recerca d'unes regles tals que permetin predir tan bé com sigui possible els resultats dels experiments físics. És impressionant en aquest cas com en són de bons els mètodes formals que poden ser utilitzats: Transformacions de símbols més o menys complicades en la pissarra d'un científic poden descriure la trajectòria dels coets o el comportament de les partícules elementals i les estrelles. El model del món del físic, les veritats del qual voldria descobrir i descriure, li ve donat des de fora mitjançant els seus instruments de mesura. En l'absència d'aquests, el físic treballa per obtenir un coneixement exacte del món amb diversos sistemes de regles, depenent de l'àrea d'estudi, les quals serveixen de criteri de decisió. Mentre que la física de cada dia se serveix de la lògica clàssica i de les mateixes lleis que funcionen en el nostre coneixement d'estar per casa, el físic de partícules necessita unes regles especials, l'anomenada *lògica quàntica*, ja que els seus experiments semblà que contradiuen el nostre sentit comú. El matemàtic estudia creacions ideals concretes i té, per tant, moltes menys limitacions a l'hora d'escollir les regles. Els llenguatges dels informàtics han de poder descriure tant les abstraccions del nostre pensament i del món que ens envolta com els sistemes físics, com són els ordinadors o els instruments de control.

Lògiques no clàssiques

Volem considerar ara la lògica no monòtona i la *lògica lineal* com dos exemples de llenguatges artificials i de sistemes de regles, els quals juguen un paper especial en la informàtica d'avui. A més, aquestes lògiques difereixen clarament de la lògica comuna i de la *lògica de predicats* tan important en la matemàtica.

En molts sistemes lògics val el principi que a partir del coneixement de nous fets podem també deduir noves conseqüències. En particular, nous fets no poden fer que conclusions prèviament establertes deixin de ser vertaderes. Volem il·lustrar això amb el famós exemple de l'estruç. Suposem que sabem «Tot ocell pot volar», i també «El pardal és un ocell» i «L'estruç és un ocell». Ara podem concluir: «El pardal pot volar» i «L'estruç pot volar». Ara descobrim que l'estruç no pot volar. Basant-nos en el nou coneixement d'aquest fet ja no podem concloure que, atès que l'estruç és un ocell, aquest pot volar. El coneixe-

ment d'un nou fet ha convertit en inadmissible una conclusió prèviament vàlida. El coneixement que és parcialment inconsistent, o més exactament, el que modifica gràcies a noves percepcions un saber ja establert, representa un problema central de la intel·ligència artificial i no és tractable amb les tècniques de la *lògica de predicats.*

Una altra declaració de la lògica de predicats és la següent implicació: suposem que sabem «Si A, aleshores B» i «Si A, aleshores C». Llavors podem concloure: «Si A, aleshores B i C».

Si ara en lloc de A posem «Plou», en lloc de B «L'aire és humit» i en lloc de C «El terra es mullarà», aleshores sembla que aquesta implicació se satisfà. Però si ara en lloc de A, vostè posa «Tinc un bitllet de 5 francs», en lloc de B «Puc comprar una barra de pa de 4 francs» i en lloc de C «Puc prendre un cafè de 3 francs», és aquesta implicació encara vàlida? El misteri queda ràpidament resolt amb la següent consideració: La lògica de predicats i en particular la implicació que hem considerat no és adequada per a descriure els canvis en les condicions. Atès que la modificació de les condicions, és però, un fenòmen comú des de l'inici dels programes d'ordinador, els informàtics s'interessen especialment per la recentment desenvolupada lògica lineal en la qual es pot formular que l'ocurrència de B gairebé «consumeix» un fet de tipus A.

Lògica i informàtica

Molts enginyers deuen sovint el seu reconeixement d'alta fiabilitat al fet que en el seu camp existeixen molt bons models matemàtics. Gràcies als més de quatre mil anys d'experiència en arquitectura i en matemàtiques, i gràcies al fet que disposem des de fa uns tres-cents anys del càlcul diferencial i integral, podem disposar ara de mètodes precisos per a l'anàlisi del comportament estàtic dels edificis. Si en el nostre segle els ponts s'enfonsen, no es pot acceptar com a vàlida l'excusa de la ignorància.

Els objectes de la informàtica es poden descriure lògicament d'una manera més senzilla que no pas el comportament de les parets sota tensions. La informàtica actual, a pesar o potser a causa del seu ràpid desenvolupament, com a ciència extremadament jove, disposa encara d'una fonamentació teòrica molt petita. Els programes, contràriament als edificis, els quals són controlats per un analista de tensions, molt sovint només es comproven en alguns pocs casos. En la pràctica, com tot usuari de la informàtica al cap del temps acaba malauradament comprovant, moltes vegades resulten defectuosos. Hi ha, però, una esperança ben fonamentada que en el futur també en la informàtica disposarem d'una fonamentació teòrica i d'una experiència més àmplia, de tal manera que les eines de la lògica formal podran ser utilitzades amb molt d'èxit.

Per a aconseguir això, per a cada objecte amb què treballem en la informàtica, hem de desenvolupar una formulació en un llenguatge lògic adequat. Aquest objectiu s'hauria d'aconseguir en pocs anys. Així, avui dia ja disposem d'una lògica molt potent per a la descripció de programes sequencials, en canvi en el terreny dels sistemes compartits i paral·lels encara s'han de resoldre algunes qüestions. Al mateix temps, s'haurien de desenvolupar mètodes que fossin útils per a la manipulació d'aquests llenguatges. Així, la longitud total del programa del sistema del transbordador espacial americà, mesurada en línies de programa arriba a més de deu millions. Mentre no hi hagi tècniques que ens permetin saber, per exemple, quines conseqüències d'un programa es deriven dels efectes d'una sola línia, no podrem desfer aquesta enorme complexitat.

El problema dels generals bizantins ha estat, per cert, investigat amb detall ja fa alguns anys. Ara ja es pot demostrar efectivament, per mitjà de tècniques lògiques, quan i com és possible un consens entre els generals. Amb dos traïdors es necessiten com a mínim cinc generals lleials, per tal que el problema tingui solució. El mètode per a solucionar-lo haurà d'esperar, però, una altra ocasió.

Clemens H. Cap és professor de mètodes formals de la Informàtica a l'Institut d'Informàtica de la Universitat de Zuric.