Univerzitet u Beogradu
Matematički fakultet

Predrag Janičić

Jedan metod za automatsko dokazivanje teorema geometrije

– magistarska teza –

Mentor: dr Zoran Lučić

Komisija:
1. Ž. Lučić (~~predsednik~~ mentor)
2. Ž. Mijajlović
3. A. Jovanović
4. A. Kron
5. D. Vidas

Odbrana: 03.07.96

Beograd
1996

U ovom radu izložen je sistem za automatsko dokazivanje geometrijskih teorema Euklid zasnovan na prvoj verziji dokazivača napisanoj na programskom jeziku PROLOG (zajednički rad Stevana Kordića i autora ovog teksta) i njenim implikacijama. U ovom tekstu prvi put se izlažu kompletan geometrijski aksiomatski sistem i sistem za izvođenje dokaza koji se koriste u sistemu Euklid, kao i njihova svojstva. Pored toga, po prvi put u ovom radu izložena su neka svojstva algoritma Euklid uključujući i tzv. teoremu o domenu.

U prvom delu izložena je precizna aksiomatika teorije $\mathcal{E}$ koja pokriva veliki deo uobičajenih geometrijskih sadržaja. Teorija $\mathcal{E}$ formulisana je u okviru predikatskog računa prvog reda i ne uključuje teoriju skupova niti teoriju realnih brojeva (čime su stvoreni neophodni preduslovi da bude potpuna). U fomulisanju aksiomatskog sistema težilo se preciznosti koju ima aksiomatika Tarskog, ali istovremeno, i tradicionalnoj formi geometrijskih tvrđenja. Kao karakteristična poddteorija teorije $\mathcal{E}$, formulisana je i konačno aksiomatizovana teorija $\mathcal{E}'$ koja uključuje tzv. pseudoneprekidnost i time takođe pokriva značajan deo uobičajenih geometrijskih sadržaja. U okviru ovog dela, izložena je i nova klasifikacija geometrijskih aksioma prilagođena specifičnom sistemu izvođenja i algoritmu za automatsko izvođenje dokaza.

U drugom delu izložen je specifičan sistem izvođenja koji omogućava dedukovanje jedne klase tvrđenja teorije $\mathcal{E}'$ i to na način koji odgovara uobičajenim izvođenjima geometrijskih dokaza. Sistem je i izgrađen sa motivacijom da formalno pokrije uobičajene geometrijske dokaze, ali može da se koristi i u drugim matematičkim teorijama. Pored toga, ovaj sistem izvođenja predstavlja i formalni okvir za zaključivanje uopšte (odnosno za jedan njegov deo), na način koji prirodnom, intuitivnom rasuđivanju odgovara više od Hilbertovog ili Gencenovog sistema.

U trećem delu prezentovan je algoritam koji može, u konačnom broju koraka, da dokaže svako tvrđenje (preciznije, bilo koje tvrđenje ili neko njemu ekvivalentno) koje je uopšte dokazivo koristići pomenutu aksiomatiku i sistem izvođenja. Taj algoritam zasnovan je, donekle, na metodi iscrpljivanja, ali usmerenoj specifičnim poretkom aksioma koje se primenjuju i takozvanim *principom graničnika*. Algoritam omogućava generisanje dokaza na prirodnom jeziku na uobičajeni način, blizak našoj intuiciji (*more geometrico*). On pokazuje da je proces prirodnog zaključivanja moguće formalizovati u geometriji, ali i u drugim matematičim

teorijama, pa i u rasuđivanju uopšte. Ovaj algoritam omogućava primene heuristika koje mogu da ubrzaju proces automatskog generisanja dokaza, kao i proširivanje geometrijskog znanja uvođenjem složenijih izvedenih koncepata (npr. mimoilazne prave, podudarnost trojki tačaka i sl.), kao i korišćenjem većeg broja geometrijskih teorema. U ovom radu, akcenat je stavljen na formalizaciju znanja i metaznanja (sistema zaključivanja), pa heuristike i slična moguća unapređenja neće biti posebno razmatrani.

U četvrom delu ukratko su prikazane verzije dokazivača Euklid na programskom jeziku PROLOG (zajednički rad Stevana Kordića i autora ovog teksta) i na programskom jeziku C. U dodatku su navedene geometrijske aksiomatike Hilberta, Tarskog i Lučića (čiju svojevrsnu kombinaciju predstavlja ovde izložena nova aksiomatika); sistemi izvođenja Mendelsona i Gencena (sa kojima je u vezi ovde izložen novi sistem) i nekoliko dokaza generisanih od strane dokazivača Euklid (C verzija).

Prijatna mi je dužnost da se na svesrdnoj pomoći u izradi magistarske teze zahvalim mentoru dr Zoranu Lučiću, kao i članovima komisije dr Žarku Mijajloviću, dr Aleksandru Jovanoviću, dr Dušku Vitasu i dr Aleksandru Kronu koji su mi brojnim sugestijama pomogli u pisanju ovog teksta. Na korisnim sugestijama i na pomoći u nabavci potrebne literature zahvaljujem se i dr Slaviši Prešiću, dr Djordju Vukomanoviću, dr Borislavu Boričiću i mr Mirjani Borisavljević. Zahvaljujem se Stevanu Kordiću, koji je izuzetno pažljivo pročitao tekst i svojim savetima pomogao mi da ga uobličim. Deo rezultata iznetih u ovoj tezi zasnovan je na zajedničkim idejama koje su se odnosile na prvu verziju dokazivača Euklid. Stevanu Kordiću se zahvaljujem i na pomoći u formulisanju tih ideja u okviru ove teze. Zahvaljujem se i svima ostalima koji su mi na bilo koji način pomogli u radu na magistarskoj tezi, a posebno mojim roditeljima na dragocenoj podršci i velikom razumevanju.

Beograd, jun 1996.

Predrag Janičić

Sadržaj

0

UVOD

Automatsko dokazivanje teorema jedan je od najznačajnijih segmenata veštačke inteligencije, koji ima ne samo teorijski, matematički značaj, već i istaknuto mesto u izgradnji ekspertnih sistema i, uopšte, sistema za automatsko odlučivanje. U nekom obliku, automatsko dokazivanje teorema počelo je da se razvija uporedo sa modernom matematičkom logikom i teorijom izračunljivosti, a ubrzano od pojave prvih računara. Dalji razvoj računarstva i novi rezultati matematičke logike mnogih značajnih matematičara (često, poput Tjuringa, angažovanih u obe discipline) bili su praćeni razvojem veštačke inteligencije i pogotovu automatske dedukcije. Prvi sistemi koji su imali atribute "inteligentnog odlučivanja" realizovani su već pedesetih godina na tadašnjim računarima malih mogućnosti. Rezultati koje su ti sistemi pružali bili su skromni, ali dovoljno značajni da nagoveste nove rezultate, nove velike poduhvate i još veća očekivanja od automatskog dokazivanja teorema. Krajem pedesetih i početkom šezdesetih godina pojavili su se, između ostalih, značajni sistemi Njuela, Šaua i Sajmona, Gilmoura, Dželerntera i drugih. Ti, pionirski sistemi za automatsko dokazivanje teorema, šezdesetih i početkom sedamdesetih godina uglavnom su potisnuti "uniformnim procedurama dokaza" kao što je Robinsonov metod rezolucije i Betov metod tabloa. Kako je vreme počelo da pokazuje suštinsku neefikasnost ovih sistema, tokom sedamdesetih godina ponovo počinju kvalitativno nova istraživanja koja su imala za cilj izgradnju dokazivača koji koriste specifičnosti konkretnih teorija, pa i pojedinih teorema koje treba dokazati. U tim istraživanjima posebno mesto davano je izgradnji heuristika koje bi popravile efikasnost procesa dokazivanja. Pored toga, mnoga istraživanja su išla i ka sistemima zaključivanja, odnosno izvođenja dokaza koji bi mogli biti upotrebljivani u raznim domenima. Osamdesetih i u prvoj polovini devedesetih godina, razvijeno je nekoliko sistema (kao što je, na primer, Vuov) koji su zasnivajući se na specifičnostima domena uspevali da postignu izuzetnu efikasnost.

U svim sistemima za automatsko dokazivanje teorema, a pogotovu u onim koji se odnose samo na jednu teoriju, izuzetno važan je izbor aksioma i pravila izvođenja kako bi bili prikladni za automatsku primenu. To je posebno izraženo u geometriji koja ima relativno veliki broj aksioma od kojih su neke veoma složene. Dodatni problem je u tome što se geometrija kao aksiomatski sistem najčešće ne uvodi sasvim precizno, pa je nejasno koje negeometrijske aksiome (logičke aksiome, aksiome aritmetike, aksiome teorije skupova) i koja pravila izvođenja

čine tzv. pretostavljenu logiku geometrije. Iz tih, ali i iz formalnih razloga koji su u vezi sa svojstvima aksiomatskih teorija (o kojima će biti reči u prvom delu ovog teksta), sistemi za automatsko dokazivanje geometrijskih sistema najčešće su ograničeni na određeni (jasno definisan) segment geometrije. Jedan od prvih (i istovremeno jedan od najznačajnijih) sistema za automatsko dokazivanje geometrijskih teorema – Dželernterova "Mašina za geometriju" (v.[Gel63]) – bio je ograničen na mali skup teorema u vezi sa podudarnošću trouglova. U ovom sistemu dokazi su ispisivani na prirodnom jeziku i to u obliku koji odgovara uobičajenim dokazima. Oni nisu zasnivani na primeni aksioma, već na primeni određenog broja izabranih teorema. Ovaj sistem bio je prilično neefikasan i pokrivao je veoma malu klasu teorema, ali je uveo nekoliko veoma značajnih novina u automatsko dokazivanje teorema – tehnike "dijagrama" i "analogije". Verovatno najefikasniji dokazivači geometrijskih teorema su sistemi zasnovani na Vuovom algoritmu (v.npr.[Ch88]). Vuov algoritam zasnovan je na činjenici da je euklidski geometrijski prostor izomorfan Dekartovom prostoru i suštinski svodi dokazivanje geometrijskih teorema na deljenje polinoma. Sistemi zasnovani na ovom algoritmu su veoma efikasni, ali ne pokrivaju sve geometrijske teoreme, ne zasnivaju dokaze na aksiomama i ne generišu uobičajene dokaze. Kineski matematičar Čou (autor verovatno najznačajnije implementacije Vuovog algoritma), 1993. godine realizovao je i jedan sistem za dokazivanje geometrijskih teorema u tradicionalnoj, uobičajenoj formi. Taj program – *Euclid* (!), zasnovan na algebarskim metodama, uspeo je da dokaže mnoštvo teorema (Paposovu, Paskalovu, Briančonovu) i, po rečima njegovog autora, verovatno je prvi sistem koji je uspeo da generiše tradicionalne dokaze netrivijalnih geometrijskih teorema.

U ovom radu biće izložen sistem za automatsko dokazivanje geometrijskih teorema Euklid koji uključuje geometrijsku aksiomatiku, specifičan sistem izvođenja dokaza, algoritam koji ih koristi i odgovarajuće programe. Aksiomatski sistem koji se izlaže precizno je definisan u okviru predikatskog računa prvog reda i pokriva veliki deo uobičajenih geometrijskih sadržaja. S jedne strane, težilo se preciznosti koju ima geometrijska aksiomatika Tarskog, a s druge, tradicionalnom obliku tvrđenja uobičajenih u geometriji više od dve i po hiljade godina. Slično, sistem izvođenja definisan je tako da odgovara uobičajenim izvođenjima geometrijskih dokaza i da pokriva što veći segment predikatskog računa. Algoritam koji koristi pomenutu aksiomatiku i sistem izvođenja zasnovan je, donekle, na metodi iscrpljivanja, ali usmerenoj specifičnim poretkom aksioma koje se primenjuju. Algoritam tokom izvođenja dokaza daje informacije o tome koja aksioma je primenjena i omogućava generisanje dokaza na prirodnom jeziku na uobičajeni način, blizak našoj intuiciji (*more geometrico*). Pored nove klasifikacije geometrijskih aksioma, algoritam implicira i nekoliko novih tehnika, između ostalih i tzv. *princip graničnika*. U razvoju sistema Euklid i u ovom tekstu teorijskim osnovama je data prednost u odnosu na pitanja heuristika koje ubrzavaju (ili mogu da ubrzaju) sam proces automatskog dokazivanja teorema. Stoga su nova geometrijska aksiomatika, poseban sistem izvođenja (primenjiv u ranim domenima) i adekvatan algoritam koji demonstrira mogućnost automatizacije procesa izvođenja dokaza, značajnije karakteristike sistema od same efikasnosti tog izvođenja. I pored toga, sistem je tako koncipiran da može biti lako proširivan novim geometrijskim teoremama (kako se dokazi ne bi izvodili do nivoa aksioma) kao i različitim heuristikama.

1

AKSIOMATIKA

1.1 Razvoj geometrijske aksiomatike

Početkom III veka pre n.e., želeći da sakupi i sistematizuje deo dotadašnjeg geometrijskog znanja, Euklid je napisao svoje remek-delo – *Elemente*. U Euklidovim *Elementima* izložien je prvi pokušaj aksiomatskog zasnivanja geometrije, ali istovremeno i bilo koje matematičke discipline. I pored nedostataka ovog aksiomatskog sistema, većina od četiri stotine šezdeset i četiri teoreme dokazana je na način besprekoran i po današnjim merilima, a *Elementi* su više od dva milenijuma smatrani "neprevaziđenim uzorom logičkog savršenstva". U duhu antičke tradicije, geometrija je vekovima bila neizostavni deo obrazovanja i neprekidno predmet interesovanja matematičara i filozofa, a u tome su Euklidovi *Elementi* sa brojnim prevodima i izdanjima imali posebnu ulogu utičući i na razvoj celokupne matematike.

Novi impuls razvoju geometrije došao je nakon što su godine (i vekovi) uzaludnog truda mnogih matematičara da dokažu V Euklidov postulat (o paralelama) pomoću preostalih aksioma, dovele do sumnje da je takav dokaz uopšte moguće izvesti. Lobačevski i Boljaj, nezavisno jedan od drugog (i to jako sličnim putevima) otkrili su, u prvoj polovini XIX veka neeuklidsku geometriju. Lobačevski i Boljaj krenuli su od negacije V Euklidovog postulata tragajući za kontradikcijom. U tom istraživanju, međutim, nisu došli do kontradikcije, već do zaključka da sistem zasnovan na negaciji V postulata i ostalim geometrijskim aksiomama i nije kontradiktoran, već predstavlja logički konzistentan sistem. Ta otkrića dovela su ne samo do uspostavljanja nove teorije - hiperboličke geometrije, već i do strožijeg zasnivanja euklidske geometrije, bitno utičući i na ostale grane matematike.

Jedna od najznačajnijih knjiga u istoriji razvoja geometrije svakako je i Hilbertova knjiga *Osnovi geometrije* (*Grundlagen der Geometrie*) koja je objavljena 1899. godine. Njegova formalistička koncepcija stvorila je preduslove za istraživanja o neprotivrečnosti i nezavisnosti aksiomatskih sistema. Geometrijska aksiomatika izneta u toj knjizi u osnovi je većine savremenih geometrijskih aksiomatskih sistema (koji su ekvivalentni i ne razlikuju se suštinski), pa takve sisteme danas zovemo i hilbertovskim.

Krajem XIX i tokom XX veka javljalo se više različitih shvatanja i zasnivanja geometrije[1].

[1] Više o razvoju geometrije i pojedinih grupa aksioma videti npr. u [Lu94].

Tako je Lie geometriju zasnivao na teoriji transformacionih grupa, Tarski je u svojim istraživanjima geometriju povezivao sa teorijom realno zatvorenih polja, a pripadnici grupe Bourbaki smatrali su da geometriju treba razmatrati isključivo kao linearnu vektorsku algebru (i u tom smislu postavili poznati zahtev "Euclid must go!").

Mi se, u ovom tekstu, nećemo baviti pitanjima "istinitosti" euklidske i neeuklidske geometrije; pitanjima "podudarnosti sa stvarnošću"; nećemo se baviti pitanjima *a priori* ili *a posteriori* poimanja prostora (v. npr. [Ru97]) - pitanjima koja su zaokupljala ili još uvek zaokupljaju pažnju mnogih matematičara i filozofa. U ovom tekstu proučavaćemo geometriju kao formalan sistem i zadovoljiti se istinitošću koja karakteriše sam proces dedukcije. U traganju za aksiomatikom[2] prikladnom za automatsko izvođenje teorema pokušaćemo da se (kada je to moguće) zadržimo na onima koja su bliska našoj intuiciji - da bismo i pored formalističkog pristupa zadržali vezu sa ljudskim iskustvom iz kojeg je geometrijska aksiomatika i proistekla. Iako je geometrijska aksiomatika motivisana našim iskustvom i intuicijom, pravićemo distancu između sintakse (i procesa formalnog izvođenja) i semantike (tj. značenja tog izvođenja u skladu sa našim uobičajenim intuitivnim predstavama).

1.2 Različiti pristupi zasnivanju geometrije

1.2.1 Na samom početku: osnovni geometrijski objekti

Zasnivanja geometrije često se razlikuju već u prvoj rečenici:

Geometrija je teorija nekog skupa $\mathcal{R}$ čije elemente $(A, B, C, ...)$ nazivamo tačkama. *Skup $\mathcal{R}$ zovemo* prostorom*; određene podskupove od $\mathcal{R}$ nazivamo* pravama *$(g, h, k, ...)$, a druge* ravnima *$(\phi, \psi, ...)$. Svojstva tačaka, pravih i ravni prostora $\mathcal{R}$ određena su aksiomama...* (Meškovski, slično Baldus, Borsuk-Šmieleva ...).

ili

Geometrija je teorija koja opisuje tri klase objekata: tačke, prave *i* ravni *i dve relacije nad njima:* podudarno *i* između... (Hilbert[3], Halstrom ...)

Iako je smisao ovih rečenica jasan, one ipak ostavljaju neka pitanja otvorenim. U prvom pristupu: ako su tačke elementi, a prave i ravni podskupovi skupa prostor, da li je incidencija o kojoj se govori u aksiomama nužno u direktnoj vezi sa skupovnim odnosima između ovih objekata?[4] I ako jeste tako, pošto se ne navodi deo teorije skupova koji se koristi, ostaju nerazjašnjeni odnosi između geometrijskih objekata kao i npr. da li neka tačka, prava ili

[2] U ovom delu rada govorimo samo o različitim sistemima aksioma smatrajući da se koristi neki od uobičajenih sistema izvođenja.

[3] Hilbert je ovakvim pristupom izbegao upotrebu teorije skupova pri uvođenju osnovnih geometrijskih objekata, ali je već krug definisao kao "ukupnost tačaka za koje ..." (v. dodatak). O jednoj mogućnosti da se u zasnivanju geometrije (odnosno jednog njenog dela) ne koristi teorija skupova biće reči u poglavlju 1.4.1.

[4] Baldus kritikuje Hilbertov sistem zbog toga što on ne zahteva direktnu vezu između incidencije i skupovnih odnosa i navodi jednostavan primer realizacije (spornog?!) sistema u kome ta veza ne bi postojala: sve tačke (iz uobičajenog skupovnog tumačenja) ostaju nepromenjene, a sve ravni "pomere se paralelno za određenu dužinu ..." I Meškovski prihvata ovu Baldusovu kritiku, ali, ako se odlučimo za formalistički pristup, to svakako nije obavezno.

ravan mogu da pripadaju nekoj tački. Nejasno deluju i odrednice "pripada", "leži, "presek" i sl, pa ostaje i pitanje izbora pogodnih simbola i termina koji označavaju incidentnost između tačaka i pravih, tačaka i ravni i pravih i ravni ("prava a pripada ravni α" ili "prava a je podskup ravni α"?).

U drugom pristupu postavlja se pitanje da li su objekti tipa prostor, ravan i prava skupovi i šta su njihovi elementi (samo tačke ili ne?). Ako prave i ravni nisu skupovi tačaka, problematično je pitanje definisanje figura kao skupova tačaka (npr. krug), kao i (između ostalih) pitanje "preseka" prave i kruga. Pored toga, u Hilbertovom sistemu nije moguće dokazati (ni opovrgnuti !) sledeće tvrđenje (kao ni mnoga slična):

Za bilo koje dve tačke A i B, tačka A ne pripada tački B.

Umesto da se traga za odgovorom na pitanje šta je sve iz teorije skupova potrebno (ili neophodno) za zasnivanje geometrije, jedno od mogućih rešenje je smatrati incidenciju jednom od tipično geometrijskih relacija koje se uvode aksiomama. Koristiti, dakle, samo termin "incidentno" (umesto termina "pripada" i "sadrži" koji imaju skupovnu konotaciju) uprkos tome što nas takav termin udaljava od uobičajene intuitivne predstave. U tom slučaju, potrebno je, umesto nasleđivanja skupovnih odnosa, uvesti dodatne definicije kojim se uvode svojstva relacije incidentno[5], odnosno aksiome poput:

Ako je tačka A incidentna pravoj a i prava a incidentna ravni α, onda je tačka A incidentna ravni α[6] .

Pored aksioma koje precizno uvode (moguće) odnose između geometrijskih objekata, nužno je prihvatiti aksiome jednakosti, kao i saglasnost jednakosti sa predikatima[7]. Dokazivanje mnogobrojnih tvrđenja (npr. "za svaki n-tougao ..." i sl.) zahteva uključivanje aksioma prirodnih brojeva, a uvođenje mere najčešće i aksioma realnih brojeva.

Opisane dileme u vezi sa izborom osnovnih geometrijskih aksioma, njihovih međusobnih odnosa i potrebnog segmenta teorije skupova izbegnute su sistemima Fordera i Tarskog. Forder je u [Fo58] izneo sistem geometrijskih aksioma u kome su osnovni objekti isključivo tačke, a prave i ravni se definišu pomoću tačaka i njihovih međusobnoh odnosa. I u sistemu Tarskog od osnovnih objekata postoje samo tačke, a aksiome koje se (u drugim aksiomatskim sistemima) odnose na prave i ravni interpretirane su preko relacija *između* i *podudarno*. Ovaj aksiomatski sistem je po ovim pitanjima (i ne samo po njima) verovatno najprecizniji, ali ne pokriva sve uobičajene geometrijske sadržaje (koji ne mogu biti formulisani bez korišćenja teorije skupova). Takođe, iako precizan, on je jako daleko od naših uobičajenih predstava i za izgradnju geometrije praktično neupotrebljiv.

[5] Poput definicije iz [Hi99, str.4] koja kaže da prava a pripada ravni α ako svaka tačka prave a pripada ravni α.

[6] Navedena aksioma, ako se u zasnivanju geometrije prihvata pristup tipa Meškovskog, može da se koristi kao tvrđenje iz teorije skupova:

$$(x \in y \wedge y \subset z) \Rightarrow x \in z .$$

[7] Možemo smatrati da u geometriji nema funkcijskih simbola, pa nije potrebna i aksioma saglasnosti jednakosti sa funkcijama. Uostalom, za svaku teoriju prvog reda postoji ekvivalentna teorija bez funkcijskih simbola.

1.2.2 Aksiome neprekidnosti

Svojstvo neprekidnosti u različitim sistemima obezbeđuje se na različite načine, ali nijedan se po svojoj jednostavnosti ne izdvaja od drugih - sažeti iskaz neizostavno povlači upotrebu komplikovanih definicija i obratno. Pored toga, većina aksiomatskih sistema (sem npr. sistema Tarskog) za obezbeđivanje neprekidnosti zahteva i uključivanje teorije prirodnih brojeva ili (segmenta) teorije skupova. Tako se za aksiomatsko uvođenje neprekidnosti u [Hi99] koriste nizovi duži (pri čemu, aksioma V_2 iz [Hi99] praktično predstavlja metatvrđenje), u [Bo60] se koristi teorija skupova, a u [Mes65] Dedekindovo svojstvo. Takođe, meru duži, koja proističe iz aksioma neprekidnosti i koja je jedan od motiva za obezbeđivanje neprekidnosti, nije moguće definisati bez teorije realnih brojeva. Zbog toga, geometrijski sistem mora da uključuje i aksiome realnih brojeva. Važno je, međutim, da se mnoga tvrđenja u geometriji (i euklidskoj i hiperboličkoj) mogu dokazati bez aksioma neprekidnosti, pa prema tome i bez upotrebe teorije realnih brojeva. Geometriju zasnovanu na aksiomama incidencije, raspореda, podudarnosti i euklidskoj aksiomi o paralelama zovemo *elementarnom (euklidskom) geometrijom*[8].

U vezi sa aksiomama neprekidnosti veoma su važni rezultati Tarskog (v. dodatak i [Ta71]) koji se odnose na (pomenutu) teoriju $\mathcal{E}_2$ – geometrijski aksiomatski sistem "bez proširenja iz teorije skupova" (koji je prilično daleko od uobičajenog "geometrijskog načina"). U tom sistemu neprekidnost je obezbeđena beskonačnom (rekurzivnom)[9] familijom aksioma određenog tipa. Za tako zasnovanu teoriju $\mathcal{E}_2$, Tarski je pokazao da je potpuna i odlučiva, ali i da ne može biti konačno aksiomatizovana, što sugeriše zaključak da bez uključivanja (dela) teorije skupova nije moguće zasnovati geometriju konačnim sistemom aksioma tako da u njoj važe svojstva neprekidnosti[10]. U jednoj varijanti svog sistema – u teoriji $\mathcal{E}_2''$, Tarski je familiju aksioma neprekidnosti zamenio jednom aksiomom kojom se (u terminima drugih aksiomatika) tvrdi da za dve tačke od kojih je jedna u unutrašnjoj, a druga u spoljašnjoj oblasti kruga postoji treća tačka koja je između njih i pripada krugu. Sa tako obezbeđenom pseudoneprekidnošću, ovaj sistem je (naravno) nepotpun, ali pokriva veliki deo uobičajenih geometrijskih sadržaja (uključujući i one koji su zasnivani na neprekidnosti).

1.3 Karakteristike geometrijskih aksiomatskih sistema

1.3.1 Tri Hilbertova zahteva

Preispitivanje Euklidove geometrije i njegovog petog postulata dovelo je do zasnivanja neeuklidske geometrije, do izgradnje prvih formalnih sistema i uticalo na celokupnu matematiku. 1899. David Hilbert je u svom delu *Osnovi geometrije* precizirao dotadašnja znanja iz domena

[8] Ovakvu definiciju elementarne geometrije koristi H.Meškovski u [Mes65]. A.Tarski, međutim, u [Ta71] elementarnu geometriju određuje kao deo euklidske geometrije koji može biti formulisan i dokazan bez upotrebe teorije skupova. Termin "elementarna" koristi se ponekad i za teorije formulisane u okvirima predikatskog računa prvog reda.

[9] Za skup **E** kažemo da je *rekurzivan* ako postoji efektivni algoritam koji u svakom pojedinačnom slučaju može da odgovori na pitanje da li dati element pripada skupu **E** ili ne. (Npr. svaki konačan skup je rekurzivan.)

[10] U poglavlju 1.4.3 biće dokazane analogne teoreme za aksiomatiku koja se uvodi u ovom radu.

geometrije i obogatio ih svojom formalističkom koncepcijom. U tom svom delu on je postavio i zahteve koje treba da ispunjava neki aksiomatski sistem (ne samo geometrijski):

I Sistem aksioma treba da bude neprotivrečan ;

II Aksiome treba da budu nezavisne ;

III Sistem aksioma treba da bude potpun .

Prvi Hilbertov zahtev znači da se od sistema aksioma očekuje da nije moguće iz njega izvesti tvrđenje $\mathcal{A}$ i tvrđenje $\neg\mathcal{A}$. Ekvivalentna je formulacija po kojoj za teoriju $\mathcal{T}$ kažemo da je *neprotivrečna* ako u njoj nije valjana svaka formula. Neprotivrečnost neke teorije može se dokazati postojanjem njenog modela[11].

Drugi Hilbertov zahtev odnosi se na *nezavisnost* aksioma – ako je neku aksiomu moguće dokazati pomoću preostalih aksioma, onda ona treba da bude izostavljena. Nezavisnost neke aksiome od ostatka sistema najčešće se dokazuje postojanjem nekog modela u kojem važe sve aksiome osim one za koju je potrebno dokazati da je nezavisna. Klasičan primer po pitanju nezavisnosti aksioma je onaj koji se odnosi na Euklidov postulat o paralelama - bilo je potrebno više od dve hiljade godina da bi se utvrdilo da Euklidov peti postulat nije moguće dokazati. Poenkareov model dokazuje da je Euklidov postulat o paralelama nezavisan od aksioma apsolutne geometrije - naime, u Poenkareovom modelu važe sve aksiome apsolutne geometrije, ali ne važi i Euklidov postulat o paralelama. Nezavisnost sistema aksioma može biti definisana i strožije (v. npr. [Mes65], [Ba37] ili [Ba38]). Dokaze tvrđenja o nezavisnosti geometrijskih aksioma videti npr. u [Hi99, str.31] ili [Bo60, str.194].

Treći Hilbertov zahtev govori o potpunosti. Neki sistem aksioma $\mathcal{S}$ zovemo *potpunim* ako je za svako pripadno[12] tvrđenje $\mathcal{A}$ tačno jedno od sledeća dva tvrđenja istinito:

$\mathcal{A}$ *sledi iz sistema aksioma* $\mathcal{S}$

$\neg\mathcal{A}$ *sledi iz sistema aksioma* $\mathcal{S}$.

Ovaj zahtev je svakako bitan, ali ne i nužan. U savremenoj matematici postoje opšte teorije važne dobrim delom baš zbog svoje nepotpunosti. (Uostalom, i izuzetno značajna, apsolutna geometrija je nepotpuna teorija.) Kažemo da je sistem aksioma *monomorfan* ili *kategoričan* ako su svaka dva njegova modela iste kardinalnosti izomorfna. Ako je sistem aksioma kategoričan, onda je on potpun. Zaista, ako pretpostavimo suprotno - da sistem

[11] *Model* je svaka struktura $\mathbf{A} = (A, R, F, C)$, gde je A neprazan skup (domen modela $\mathbf{A}$, R je skup relacija nad A, F je skup operacija nad A i C je skup konstanti.

Neka je L jezik prvog reda. Pod *interpretacijom* jezika L u modelu $\mathbf{A}$ podrazumevamo preslikavanje I sa domenom L, takvo da važi:

-ako r pripada skupu predikatskih simbola jezika L, tada je $I(r)$ relacija modela $\mathbf{A}$ dužine $ar(r)$;
-ako f pripada skupu funkcijskih simbola jezika L, tada je $I(f)$ operacija modela $\mathbf{A}$ dužine $ar(f)$;
-ako c pripada skupu simbola konstanti jezika L, tada $I(c)$ pripada A.

Svaka interpretacija jezika L u skupu A određuje jedinstven model $\mathbf{A} = (A, I(R_L), I(F_L), I(C_L))$. Ovako uveden model označavamo kraće $\mathbf{A}) = (A, I)$.

Neka je L jezik teorije $\mathcal{T}$. Za model $\mathbf{A} = (A, I)$ kažemo da je *model teorije* $\mathcal{T}$, ako su u njemu tačne sve aksiome teorije $\mathcal{T}$ (v.[Mi87]).

[12] *Pripadnim* zovemo tvrđenja koja sadrže samo takve pojmove i relacije koji se već nalaze u sistemu aksioma.

aksioma teorije $\mathcal{T}$ nije potpun, to znači da postoji neko tvrđenje $\mathcal{A}$ koje nije moguće ni dokazati ni opovrgnuti. Tada možemo skup aksioma teorije $\mathcal{T}$ proširiti tvrđenjima $\mathcal{A}$, odnosno $\neg\mathcal{A}$ kao aksiomama i time dobiti dve neprotivrečne (ako je $\mathcal{T}$ neprotivrečna) teorije $\mathcal{T}'$ i $\mathcal{T}''$. Neka su $\mathcal{M}'$ i $\mathcal{M}''$ modeli ovih teorija. Svaki od njih je, svakako, i model teorije $\mathcal{T}$, ali kako u $\mathcal{T}'$ važi $\mathcal{A}$, a u $\mathcal{T}''$ važi $\neg\mathcal{A}$, zaključujemo da modeli $\mathcal{M}'$ i $\mathcal{M}''$ teorije $\mathcal{T}$ nisu izomorfni. Dakle, ako teorija nije potpuna ona nije kategorična (v. [Po63, str.55]). Može se (korišćenjem dekartovskog modela) dokazati da je uobičajeni sistem geometrijskih aksioma kategoričan (dokaz videti npr. u [Bo60, str.277]), što i dalje ne znači da je tako zasnovana teorija potpuna, jer ona, pored geometrijskih aksioma, uključuje i (neke) aksiome teorije skupova i aksiome teorije realnih brojeva.

Za većinu geometrijskih aksiomatika teško je (ili nemoguće) odgovoriti na pitanje da li one zadovoljavaju navedene Hilbertove zahteve iz razloga što najčešće nije precizirano šta sve one uključuju, tj. šta predstavlja tzv. *pretpostavljenu logiku*, što se ne definiše skup formula teorije, kao ni sistem izvođenja koji se koristi (dokazi se obično izvode intuitivno, neformalno). Tako, za Hilbertov aksiomatski sistem možemo da konstatujemo ili da je neprecizan – jer nema definisan skup formula ili da je nepotpun – jer se u njemu ne mogu ni dokazati ni opovrgnuti neka tvrđenja[13] (v. poglavlje 1.2.1). Za geometrijske sisteme drugačijeg tipa – za sisteme koji koriste deo teorije skupova, ne kaže se koji je to deo, pa se i ne može precizno govoriti o svojstvima tako zasnovane geometrije. Geometrijski sistemi koji bi uključivali celu teoriju skupova ne bi bili potpuni, jer kako je aritmetika, na osnovu Gedelovih rezultata, esencijalno nepotpuna[14](v. npr. [Mi86,str.58]), onda je i svaka aksiomatska teorija koja sadrži aritmetiku takođe (esencijalno) nepotpuna. Teorija skupova sadrži aritmetiku, pa je geometrija koja uključuje teoriju skupova (esencijalno) nepotpuna teorija. Upravo u tome i jeste smisao traganja za geometrijskom aksiomatikom koja ne uključuje teoriju skupova, iako u takvoj teoriji nije moguće formulisati (i dokazati) sve teoreme geometrije koja uključuje teoriju skupova (mada je moguće formulisati značajan njen segment). Zaista, geometrija može biti formulisana bez teorije skupova tako da bude potpuna teorija i tako da pokriva veliki deo uobičajenih geometrijskih sadržaja. Kako je potpuna teorija sa rekurzivnim skupom aksioma odlučiva (v. poglavlje 1.3.2), takav pristup ima izuzetan značaj i u teoriji izračunljivosti i u oblasti automatskog dokazivanja teorema.

1.3.2 Odlučivost aksiomatske teorije

Nakon Hilbertovih zahteva, pomenućemo još jedno važno pitanje vezano za aksiomatske teorije – pitanje odlučivosti teorije i pokušati da delimično odgovorimo na njega kada je reč o euklidskoj geometriji.

Za teoriju $\mathcal{T}$ kažemo da je *odlučiva* ako postoji efektivni algoritam koji za svaki pojedinačni iskaz $\mathcal{A}$ te teorije može da odgovori na pitanje da li je on dokaziv u teoriji $\mathcal{T}$ ili nije. Ako takav

[13] Hilbertov sistem formulisan je 1899. godine, dakle, pre nego što je precizno definisan predikatski račun. Zanimljivo je, međutim, da ni u redigovanom izdanju, objavljenom 1956. u redakciji Pola Bernajsa, ovo nije ispravljeno, pa čak ni prokomentarisano.

[14] Za teoriju kažemo da je *esencijalno nepotpuna* ako je svako njeno neprotivrečno proširenje nepotpuna teorija.

algoritam ne postoji, za teoriju kažemo da je *neodlučiva*. Pojam odlučivosti je, očigledno, veoma važan i za oblast automatskog dokazivanja teorema. Naime, za odlučivu teoriju postoji efektivna procedura (pa i algoritmi i programi) koji za svako tvrđenje mogu da utvrde da li je teorema ili nije. Takve procedure su, međutim, zbog svoje složenosti i neefikasnosti, najčešće neprimenljive u praksi, ali ipak, bar "u principu" daju rešenje problema.

Naglasimo da se pojmovi odlučivosti i potpunosti bitno razlikuju i da postoje teorije koje su potpune, ali nisu odlučive i one koje su odlučive, ali nisu potpune. Vezu između potpunih i odlučivih teorija određuje sledeća važna teorema (v.[Ta69, str.14]):

Potpuna teorija $\mathcal{T}$ sa standardnom formalizacijom je odlučiva akko je aksiomatibilna[15].

Za svoj geometrijski sistem $\mathcal{E}_2$, izgrađen bez uključivanja teorije skupova, Tarski je dokazao da je potpun, pa na osnovu navedene teoreme i odlučiv, i postavio hipotezu da nijedna njena konačno aksiomatizovana podteorija nije odlučiva (v.poglavlje 1.4.3). Tarski je u [Ta71, str.172] formulisao i teoriju $\mathcal{E}'_2$, koja se od teorije $\mathcal{E}_2$ razlikuje se po tome što u shemi aksioma neprekidnosti dopušta i upotrebu "malog segmenta teorije skupova" - upotrebu skupova sa proizvoljnim konačnim brojem tačaka. Za teoriju $\mathcal{E}'_2$ koja je šira od $\mathcal{E}_2$ i pokriva više uobičajenih geometrijskih iskaza (npr. za poligone sa proizvoljnim brojem temena i sl.) Tarski je pokazao da je neodlučiva, i štaviše, da je neodlučivo svako njeno neprotivrečno proširenje. Ovaj rezultat sugeriše i hipotezu da ne može biti formulisan odlučiv geometrijski sistem koji uključuje teoriju skupova ili njen deo.

1.4 Aksiomatika euklidske geometrije u sistemu EUKLID

Aksiomatika euklidske geometrije koja će ovde biti izložena proistekla je iz koncepta dokazivača geometrijskih teorema EUKLID (v.[JK95a], [JK95b]). Prirodom dokazivača određena je stroga struktura aksioma, ali i njihova nova klasifikacija. Ova aksiomatika ne uključuje teoriju skupova, ali i pored toga, zadržava, u velikoj meri, pristup *more geometrico*. Jedna varijanta sistema – teorija $\mathcal{E}'$ ograničena je na euklidsku geometriju sa tzv. pseudoneprekidnošću (v.poglavlje 1.2.2) – na segment koji pokriva veliki deo uobičajenih geometrijskih sadržaja.

1.4.1 Teorija $\mathcal{E}$ - osnovni pojmovi i aksiomatski sistem

U zanivanju geometrije (teorije $\mathcal{E}$) koristimo uobičajene logičke simbole $\vee$, $\wedge$, $\neg$, $\Rightarrow$, $\forall$ i $\exists$; simbole $x_1, x_2, x_3, \ldots$ za promenljive; simbole $a_1, a_2, a_3, \ldots$ za (uvedene) konstante i simbole $\mathcal{S}$ za jednoelementni predikat *je tačka*, $\mathcal{L}$ za jednoelementni predikat *je prava*, $\mathcal{P}$ za jednoelementni predikat *je ravan*, $=$ (u infiksnom zapisu) za dvoelementni predikat *identično*, $\mathcal{I}$ za dvoelementni predikat *incidentno*, $\mathcal{B}$ za troelementni predikat *između* i $\mathcal{C}$ ili $\cong$ (u infiksnom zapisu) za četvoroelementni predikat *podudarno*[16].

[15] Za teoriju $\mathcal{T}$ kažemo da je *sa standardnom formalizacijom* ako može biti zasnovana u okviru predikatskog računa pravog reda sa jednakošću.

Za teoriju $\mathcal{T}$ kažemo da je *aksiomatibilna* ako postoji rekurzivan skup A dokazivih iskaza iz $\mathcal{T}$ takvih da je svaki iskaz dokaziv u $\mathcal{T}$ dokaziv i iz skupa A, tj. ako postoji rekurzivan skup aksioma za teoriju $\mathcal{T}$.

[16] Opisani koncept zasnivanja geometrije može se nadgraditi aksiomatskim uvođenjem i drugih "tipova" geometrijskih objekata. Svojstva geometrijskih objekata kao što su duž, trougao, krug, unutrašnjost kruga,

predikat	čitamo
$\mathcal{S}(a)$	a je tačka
$\mathcal{L}(b)$	b je prava
$\mathcal{P}(c)$	c je ravan
$a = b$	a je identično b
$\mathcal{I}(a,b)$	a je incidentno b
$\mathcal{B}(a,b,c)$	b je između a i c
$\mathcal{C}(a,b,c,d)$	(a,b) je podudarno sa (c,d)
$((a,b) \cong (c,d)$	(a,b) je podudarno sa $(c,d))$
$kolin(a,b,c)$	a, b i c su kolinearne
$kompl(a,b,c,d)$	a, b, c i d su komplanarne
$seku\_se(a,b)$	a i b se seku

Tabela 3.1. Spisak (osnovnih i izvedenih) predikata u sistemu EUKLID

Definišimo pojam formule teorije $\mathcal{E}$[17]:

Definicija1.1 :

Ako su t_1 i t_2 promenljive ili konstante, onda je $t_1 = t_2$ atomička formula; Ako su t_1 i t_2 promenljive ili konstante, onda je $\mathcal{I}(t_1, t_2)$ atomička formula; Ako su t_1, t_2 i t_3 promenljive ili konstante, onda je $\mathcal{B}(t_1, t_2, t_3)$ atomička formula. Ako su t_1, t_2, t_3 i t_4 promenljive ili konstante, onda je $(t_1, t_2) \cong (t_3, t_4)$ atomička formula.

Definicija1.2 :

(1) Ako je $\mathcal{A}$ atomička formula onda su formule $\mathcal{A}$ i $\neg\mathcal{A}$ literali.

(2) Izraz je literal samo ako može biti dobijen na osnovu pravila (1).

Definicija1.3 :

(1) Svaka atomička formula je formula.

(2) Ako su $\mathcal{A}_1$ i $\mathcal{A}_2$ formule i x promenljiva, onda su formule i $(\neg\mathcal{A}_1)$, $(\mathcal{A}_1 \wedge \mathcal{A}_2)$, $(\mathcal{A}_1 \vee \mathcal{A}_2)$, $(\mathcal{A}_1 \Rightarrow \mathcal{A}_2)$, $((\forall x)\mathcal{A}_1)$ i $((\exists x)\mathcal{A}_1)$[18].

poluprava, pramen pravih itd. uvodila bi se aksiomama. Na taj način, bez upotrebe teorije skupova, povećava se segment "tradicionalne" geometrije pokriven ovako zasnovanom teorijom. Aksiomatsko uvođenje više geometrijskih objekata ima opravdanje jer (*i*) na ovaj način, bez upotrebe teorije skupova, može da se pokrije veliki deo uobičajenih geometrijskih sadržaja i pri tom je, u velikoj meri, moguće zadržati direktnu vezu sa tradicionalnim pristupom; (*ii*) u tradicionalnom pristupu, u skladu sa određenom motivacijom, definišu se određeni pojmovi, a zatim se dokazuje da oni zadovoljavaju "željena" svojstva; na ovaj način aksiomatski se obezbeđuju svojstva koja želimo da imaju određeni geometrijski objekti; (*iii*) i u većini tradicionalnih aksiomatskih sistema prava i ravan se uvode aksiomatski iako ih je moguće definisati; (*iv*) ovako izgrađen aksiomatski sistem i dalje bi imao svojstvo nezavisnosti aksioma.

[17] U teoriji $\mathcal{E}$ nema funkcijskih simbola, pa je definicija formule teorije $\mathcal{E}$ nešto jednostavnija od opšte definicije. Iz istog razloga, među aksiomama nema aksiome saglasnosti jednakosti sa funkcijama.

[18] Zagrade možemo da izostavljamo u skladu sa uobičajenim konvencijama.

(3) Izraz je formula samo ako može biti dobijen na osnovu pravila (1) i (2).

Formulu $a = b$ čitamo *geometrijski objekti a i b su identični.* Formulu $\neg(a = b)$ zapisujemo drugačije $a \neq b$ i čitamo *geometrijski objekti a i b su različiti.* Formulu $\mathcal{I}(a, b)$ čitamo *geometrijski objekat a incidentan je geometrijskom objektu b.* Formulu $\mathcal{B}(a, b, c)$ čitamo *geometrijski objekat b je između geometrijskih objekata a i c.* Formulu $\mathcal{C}(a, b, c, d)$ (odnosno $(a, b) \cong (c, d)$) čitamo *par geometrijskih objekata a, b podudaran je paru geometrijskih objekata c, d.*

Usvajamo i dogovor po kojem ćemo sintagme tipa
Za geometrijski objekat a za koji važi $\mathcal{S}(a)$ ...
(i slične) zamenjivati kraćim sintagmama tipa:
Za tačku a ...

Za pojmove *valjana* i *kontradiktorna* formula, kao i *dokaziva* formula, odnosno *teorema*[19] prihvatamo uobičajene definicije (v.npr.[Men64, str.29]). Na osnovu teoreme o potpunosti predikatskog računa, svaka valjana formula teorije $\mathcal{E}$ je teorema i obratno.

Osobine osnovnih geometrijskih predikata uvodimo aksiomama. Prvu grupu čine tzv. *aksiome zasnovanosti*, kojima se uvode "tipovi geometrijskih objekata" i opseg osnovnih relacija[20].

Aksiome zasnovanosti

$\mathcal{Z}_1$: (Aksioma razdvajanja) Za svaki geometrijski objekat važi tačno jedna od relacija *je tačka, je prava* ili *je ravan.*

$$\forall x((\mathcal{S}(x) \wedge \neg\mathcal{L}(x) \wedge \neg\mathcal{P}(x)) \vee (\neg\mathcal{S}(x) \wedge \mathcal{L}(x) \wedge \neg\mathcal{P}(x)) \vee (\neg\mathcal{S}(x) \wedge \neg\mathcal{L}(x) \wedge \mathcal{P}(x))).$$

(Aksiome opsega)
$\mathcal{Z}_2 : \forall x\forall y(\neg(\mathcal{S}(x) \wedge \mathcal{S}(y)) \wedge \neg(\mathcal{L}(x) \wedge \mathcal{L}(y)) \wedge \neg(\mathcal{P}(x) \wedge \mathcal{P}(y)) \Rightarrow \neg(x = y))$
$\mathcal{Z}_3 : \forall x\forall y(\neg(\mathcal{S}(x) \wedge \mathcal{L}(y)) \wedge \neg(\mathcal{S}(x) \wedge \mathcal{P}(y)) \wedge \neg(\mathcal{L}(x) \wedge \mathcal{P}(y)) \Rightarrow \neg\mathcal{I}(x, y))$
$\mathcal{Z}_4 : \forall x\forall y\forall z(\neg\mathcal{S}(x) \vee \neg\mathcal{S}(y) \vee \neg\mathcal{S}(z) \Rightarrow \neg\mathcal{B}(x, y, z))$
$\mathcal{Z}_5 : \forall x\forall y\forall z\forall u(\neg\mathcal{S}(x) \vee \neg\mathcal{S}(y) \vee \neg\mathcal{S}(z) \vee \neg\mathcal{S}(u) \Rightarrow \neg(x, y) \cong (z, u))$

Aksiome jednakosti i saglasnosti

$\mathcal{J}_1 : \forall x\,(x = x)$
$\mathcal{J}_2 : \forall x\,\forall y\,(x = y \Rightarrow y = x)$
$\mathcal{J}_4 : \forall x_1\forall x_2 \ldots \forall x_n\forall y\ (x_i = y \wedge \Phi(x_1, x_2, \ldots, x_i, \ldots, x_n) \Rightarrow \Phi(x_1, x_2, \ldots, y, \ldots, x_n))$,
gde je $\Phi(x_1, x_2, \ldots, x_i, \ldots, x_n)$ literal[21].

Zbog jednostavnosti, za zapis preostalih aksioma umesto navedenog skupa simbola koristićemo tri tipa simbola za promenljive: velika latinična slova $X, X_1, X_2, \ldots, Y, Z, \ldots$ (intu-

[19] U dokazivaču EUKLID koristi se specifičan sistem izvođenja, ali u ovom delu rada, dok govorimo o svojstvima teorije $\mathcal{E}$, smatraćemo da se koristi neki od uobičajenih sistema izvođenja (v.npr.[Men64, str.57]).

[20] U dokazivaču EUKLID aksiome zasnovanosti koriste se implicitno.

[21] Naglasimo da se time saglasnost ne uvodi kao shema, već kao konačan niz aksioma. U samom dokazivaču, kao aksiome se, zbog pojednostavljivanja dokaza, koriste i tvrđenja o saglasnosti jednakosti sa definisanim predikatima koje se koriste u dokazivaču (v. tabelu 3.1).

itivno za tačke), mala latinična slova $x, x_1, x_2, \ldots, y, z, \ldots$ (intuitivno za prave) i grčka slova $\phi, \phi_1, \phi_2, \ldots, \chi, \psi, \ldots$ (intuitivno za ravni); kao i odgovarajuća tri tipa simbola za (uvedene) konstante: $A, A_1, A_2, \ldots, B, C, \ldots$; $a, a_1, a_2, \ldots, b, c, \ldots$ i $\alpha, \alpha_1, \alpha_2, \ldots, \beta, \gamma, \ldots$. Npr. koristeći navedene simbole pisaćemo $\exists X \mathcal{A}(X)$ (gde je $\mathcal{A}$ neka formula) umesto (u najpre uvedenom jeziku) $\exists x(\mathcal{S}(x) \wedge \mathcal{A}(x))$, $\forall X \mathcal{A}(X)$ umesto $\forall x(\mathcal{S}(x) \Rightarrow \mathcal{A}(x))$, $\mathcal{A}(\alpha)$ umesto $\neg \mathcal{P}(a) \vee \mathcal{A}(a)$ i sl.

Većina preostalih aksioma zasnovana je na aksiomatskom sistemu iz [Lu94]. Oznake aksioma u uglastim zagradama predstavljaju oznake aksioma iz tog sistema. Aksioma $\mathcal{N}_1$ se ne pojavljuje u pomenutom sistemu, a aksioma $\mathcal{N}_2$ predstavlja jaču varijantu aksiome paralelnosti (v. aksiomu paralelnosti iz [Hi99, str.26] i teoremu 26.1 iz [Lu94, str.204]), pa su za njih oznake u uglastim zagradama izostavljene. Kao adekvatnije za automatsko dokazivanje geometrijskih teorema, u aksiomatski sistem $\mathcal{E}$ umesto aksiome $I2$ iz [Lu94] uvrštena je nešto slabija aksioma $\mathcal{P}_4$, a umesto $I9$ nešto jača aksioma $\mathcal{JP}_1$. Umesto aksiome $I7$ iz [Lu94], koristi se modifikovna varijanta – aksioma $\mathcal{N}_{12}$ (koja je u skladu sa aksiomom $\mathcal{N}_1$). Aksioma $III5$ iz [Lu94] razdvojena je na aksiome $\mathcal{N}_{13}$ i $\mathcal{P}_9$, a aksioma $III6$ na aksiome $\mathcal{P}_1$ i $\mathcal{P}_2$.

Navedimo najpre definicije koje, zbog jednostavnijeg zapisa, koristimo u formulaciji geometrijskih aksioma:

Tri tačke X, Y i Z su kolinearne *ako i samo ako su incidentne nekoj pravoj x.*

$$\forall X \forall Y \forall Z \exists x(kolin(X,Y,Z) \Rightarrow (\mathcal{I}(X,x) \wedge \mathcal{I}(Y,x) \wedge \mathcal{I}(Z,x)))$$

$$\forall X \forall Y \forall Z \forall x((\mathcal{I}(X,x) \wedge \mathcal{I}(Y,x) \wedge \mathcal{I}(Z,x)) \Rightarrow kolin(X,Y,Z))$$

Četiri tačke X, Y, Z i U su komplanarne *ako i samo ako su incidentne nekoj pravoj ϕ.*

$$\forall X \forall Y \forall Z \forall U \exists \phi(kompl(X,Y,Z,U) \Rightarrow (\mathcal{I}(X,\phi) \wedge \mathcal{I}(Y,\phi) \wedge \mathcal{I}(Z,\phi) \wedge \mathcal{I}(U,\phi)))$$

$$\forall X \forall Y \forall Z \forall U \forall \phi((\mathcal{I}(X,\phi) \wedge \mathcal{I}(Y,\phi) \wedge \mathcal{I}(Z,\phi) \wedge \mathcal{I}(U,\phi)) \Rightarrow kompl(X,Y,Z))$$

Dve prave x i y se seku *ako i samo ako postoji tačka X koja je incidentna i jednoj i drugoj.*

$$\forall x \forall y \exists X(seku\_se(x,y) \Rightarrow (\mathcal{I}(X,x) \wedge \mathcal{I}(X,y)))$$

$$\forall x \forall y \forall X((\mathcal{I}(X,x) \wedge \mathcal{I}(X,y)) \Rightarrow seku\_se(x,y))$$

Prava x i ravan ϕ se seku *ako i samo ako postoji tačka X koja je incidentna i jednoj i drugoj.*

$$\forall x \forall \phi \exists X(seku\_se(x,\phi) \Rightarrow (\mathcal{I}(X,x) \wedge \mathcal{I}(X,\phi)))$$

$$\forall x \forall \phi \forall X((\mathcal{I}(X,x) \wedge \mathcal{I}(X,\phi)) \Rightarrow seku\_se(x,\phi))$$

Dve ravni ϕ i ψ se seku *ako i samo ako postoji tačka X koja je incidentna i jednoj i drugoj.*

$$\forall \phi \forall \psi \exists X(seku\_se(\phi,\psi) \Rightarrow (\mathcal{I}(X,\phi) \wedge \mathcal{I}(X,\psi)))$$

$$\forall\phi\forall\psi\forall X((\mathcal{I}(X,\phi)\wedge\mathcal{I}(X,\psi))\Rightarrow seku\_se(\phi,\psi))$$

Neproduktivne aksiome

$\mathcal{N}_1$: [22] Ako je tačka X incidentna pravoj x, i prava x incidentna ravni ϕ, onda je tačka X incidentna ravni ϕ.

$$\forall X\forall x\forall\phi(\mathcal{I}(X,x)\wedge\mathcal{I}(x,\phi)\Rightarrow\mathcal{I}(X,\phi))$$

$\mathcal{N}_2$: Za svaku pravu x, svaku tačku X i svaku ravan ϕ takve da je tačka X incidentna ravni ϕ, a nije incidentna pravoj x i da je prava x incidentna ravni ϕ, postoji najviše jedna prava incidentna ravni ϕ takva da joj je incidentna tačka X, a ne seče se sa pravom x, nije joj incidentna nijedna tačka koja je incidentna pravoj x.

$$\forall x\forall X\forall\phi\forall y\forall z(\neg\mathcal{I}(X,x)\wedge\mathcal{I}(X,\phi)\wedge\mathcal{I}(x,\phi)\wedge\mathcal{I}(X,y)\wedge\mathcal{I}(X,z)\wedge\mathcal{I}(y,\phi)\wedge\mathcal{I}(z,\phi)$$

$$\wedge\neg seku\_se(x,y)\wedge\neg seku\_se(x,z)\Rightarrow y=z)$$

$\mathcal{N}_3$: [$III1$] Ako su X,Y,Z,U tačke takve da je $(X,Y)\cong(Z,U)$ i $X=Y$, tada je $Z=U$.

$$\forall X\forall Y\forall Z\forall U((X,Y)\cong(Z,U)\wedge X=Y\Rightarrow Z=U)$$

$\mathcal{N}_4$: [$III3$] Ako su X,Y,Z,U,V,W tačke takve da je $(X,Y)\cong(Z,U)$ i, uz to, $(X,Y)\cong(V,W)$ tada je $(Z,U)\cong(V,W)$.

$$\forall X\forall Y\forall Z\forall U\forall V\forall W((X,Y)\cong(Z,U)\wedge(X,Y)\cong(V,W)\Rightarrow(Z,U)\cong(V,W))$$

$\mathcal{N}_5$: [$III7$] Ako su X,Y,Z,X',Y' i Z' tačke takve da važi $\mathcal{B}(X,Z,Y)$ i $\mathcal{B}(X',Z',Y')$ i $(X,Z)\cong(X',Z')$ i $(Y,Z)\cong(Y',Z')$ tada je i $(X,Y)\cong(X',Y')$.

$$\forall X\forall Y\forall Z\forall X'\forall Y'\forall Z'(\mathcal{B}(X,Z,Y)\wedge\mathcal{B}(X',Z',Y')\wedge(X,Z)\cong(X',Z')\wedge(Y,Z)\cong(Y',Z')$$

$$\Rightarrow(X,Y)\cong(X',Y'))$$

$\mathcal{N}_6$: [$II1$] Ako za tačke X,Y i Z važi $\mathcal{B}(X,Y,Z)$ tada su one različite kolinearne tačke.

$$\forall X\forall Y\forall Z(\mathcal{B}(X,Y,Z)\Rightarrow X\neq Y\wedge Y\neq Z\wedge Z\neq X\wedge kolin(x,y,z))$$

$\mathcal{N}_7$: [$II2$] Ako je $\mathcal{B}(X,Y,Z)$ tada je $\mathcal{B}(Z,Y,X)$.

$$\forall X\forall Y\forall Z(\mathcal{B}(X,Y,Z)\Rightarrow\mathcal{B}(Z,Y,X))$$

$\mathcal{N}_8$: [$II3$] Ako je $\mathcal{B}(X,Y,Z)$ tada nije $\mathcal{B}(X,Z,Y)$.

$$\forall X\forall Y\forall Z(\mathcal{B}(X,Y,Z)\Rightarrow\neg\mathcal{B}(X,Z,Y))$$

[22] U odnosu na uobičajene aksiomatske sisteme ova aksioma je kvalitativno nova $\mathcal{N}_1$. Po standardnoj klasifikaciji ova aksioma bila bi uvrštena u grupu aksioma incidencije.

$\mathcal{N}_9$: $[III2]$ Ako su X i Y bilo koje dve tačke tada je $(X,Y) \cong (Y,X)$.

$$\forall X \forall Y ((X,Y) \cong (Y,X))$$

$\mathcal{N}_{10}$: $[I3]$ Postoji najviše jedna prava kojoj su incidentne dve različite tačke.

$$\forall X \forall Y \forall x \forall y (X \neq Y \mathcal{I}(X,x) \wedge \mathcal{I}(Y,x) \wedge \mathcal{I}(X,y) \wedge \mathcal{I}(Y,y) \Rightarrow x = y))$$

$\mathcal{N}_{11}$: $[I6]$ Postoji najviše jedna ravan kojoj su incidentne tri nekolinearne tačke.

$$\forall X \forall Y \forall Z \forall \phi \forall \psi (\neg kolin(X,Y,Z) \wedge \mathcal{I}(X,\phi) \wedge \mathcal{I}(Y,\phi) \wedge \mathcal{I}(Z,\phi) \wedge \mathcal{I}(X,\psi) \wedge \mathcal{I}(Y,\psi) \wedge \mathcal{I}(Z,\psi)$$

$$\Rightarrow \phi = \psi))$$

$\mathcal{N}_{12}$: $[I7]$ Ako su dve različite tačke, koje su incidentne nekoj pravoj, incidentne nekoj ravni, onda je ta incidentna istoj ravni.

$$\forall X \forall Y \forall x \forall \phi (X \neq Y \wedge \mathcal{I}(X,x) \wedge \mathcal{I}(Y,x) \wedge \mathcal{I}(X,\phi) \wedge \mathcal{I}(Y,\phi) \Rightarrow \mathcal{I}(Z,x))$$

$\mathcal{N}_{13}$: $[III5]$ Ako su X i Y dve različite tačke i tačke Z, U_1 i U_2 incidentne nekoj pravoj x, takve da su tačke U_1 i U_2 različite i važi $(X,Y) \cong (Z,U_1)$ i $(X,Y) \cong (Z,U_2)$ onda važi i $\mathcal{B}(U_1,Z,U_2)$.

$$\forall X \forall Y \forall Z \forall U_1 \forall U_2 \forall x (X \neq Y \wedge \mathcal{I}(Z,x) \wedge U_1 \neq U_2 \wedge$$

$$\mathcal{I}(U_1,x) \wedge \mathcal{I}(U_2,x) \wedge (X,Y) \cong (Z,U_1) \wedge (X,Y) \cong (Z,U_2) \Rightarrow \mathcal{B}(U_1,Z,U_2)$$

$\mathcal{N}_{14}$: $[III7]$ Ako su X,Y,Z i X_1,Y_1,Z_1 dve trojke nekolinearnih tačaka, x i x_1 prave kojima su incidentne tačke X i Y, odnosno X_1 i Y_1 i ako su U i U_1 tačke incidentne pravama x, odnosno x_1 takve da je $(X,Y) \cong (X_1,Y_1)$, $(Y,Z) \cong (Y_1,Z_1)$, $(Z,X) \cong (Z_1,X_1)$ i $(Y,U) \cong (Y_1,U_1)$ tada je i $(X,U) \cong (X_1,U_1)$.

$$\forall X \forall Y \forall Z \forall U \forall x \forall X_1 \forall Y_1 \forall Z_1 \forall U_1 \forall x_1 (\mathcal{I}(X,x) \wedge \mathcal{I}(Y,x) \wedge \neg \mathcal{I}(Z,x) \wedge \mathcal{I}(U,x) \wedge$$

$$\mathcal{I}(X_1,x_1) \wedge \mathcal{I}(Y_1,x_1) \wedge \neg \mathcal{I}(Z_1,x_1) \wedge \mathcal{I}(U_1,x_1) \wedge (X,Y) \cong (X_1,Y_1) \wedge (Y,Z) \cong (Y_1,Z_1) \wedge$$

$$(Z,X) \cong (Z_1,X_1) \wedge (Y,U) \cong (Y_1,U_1) \Rightarrow (X,U) \cong (X_1,U_1)$$

Granajuće aksiome

$\mathcal{G}_1$: $[II5]$ Ako su X,Y,Z tri kolinearne tačke od kojih svake dve nisu identične tada je $\mathcal{B}(X,Y,Z)$ ili $\mathcal{B}(Y,Z,X)$ ili $\mathcal{B}(Z,X,Y)$.

$$\forall X \forall Y \forall Z (X \neq Y \wedge Y \neq Z \wedge Z \neq X \wedge kolin(X,Y,Z) \Rightarrow \mathcal{B}(X,Y,Z) \vee \mathcal{B}(Y,Z,X) \vee \mathcal{B}(Z,X,Y))$$

$\mathcal{G}_2$: $[II6]$ Ako su X,Y,Z tri nekolinearne tačke incidentne ravni ϕ, x prava koja je incidentna ravni ϕ i nije joj incidentna tačka X, i U tačka koja je incidentna pravoj x, takva

da je $\mathcal{B}(Y,U,Z)$, tada je pravoj x incidentna tačka V, takva da je $\mathcal{B}(Z,V,X)$ ili tačka W, takva da je $\mathcal{B}(X,W,Y)$.

$$\forall X\forall Y\forall Z\forall\phi\forall x\forall U\exists V\exists W(\mathcal{I}(X,\phi)\wedge\mathcal{I}(Y,\phi)\wedge\mathcal{I}(Z,\phi)\wedge\mathcal{I}(x,\phi)\wedge\neg\mathcal{I}(X,x)\wedge\mathcal{I}(U,x)\wedge\mathcal{B}(Y,U,Z)\Rightarrow$$
$$(\mathcal{B}(Z,V,X)\wedge\mathcal{I}(V,x))\vee(\mathcal{B}(X,W,Y)\wedge\mathcal{I}(W,x)))$$

Produktivne aksiome

$\mathcal{P}_1$: $[III6]$ Ako su X,Y,Z tri nekolinearne tačke i X',Y' tačke incidentne nekoj ravni ϕ takve da je da je $(X,Y)\cong(X',Y')$, tada postoje tačke Z_1' i Z_2' incidentne ravni ϕ takve da je $(X,Z)\cong(X',Z_1')$, $(Y,Z)\cong(Y',Z_1')$ i $(X,Z)\cong(X',Z_2')$, $(Y,Z)\cong(Y',Z_2')$.

$$\forall X\forall Y\forall Z\forall X'\forall Y'\forall\phi\exists Z_1'\exists Z_2'(\neg kolin(X,Y,Z)\wedge\mathcal{I}(X',\phi)\wedge\mathcal{I}(Y',\phi)\wedge(X,Y)\cong(X',Y')\Rightarrow$$
$$(X,Z)\cong(X',Z_1')\wedge(Y,Z)\cong(Y',Z_1')\wedge(X,Z)\cong(X',Z_2')\wedge(Y,Z)\cong(Y',Z_2'))$$

$\mathcal{P}_2$: $[III6]$ Ako su tačke X,Y,Z_1 i Z_2 incidentne nekoj ravni ϕ, takve da su X i Y različite i incidentne nekoj pravoj x, Z_1 i Z_2 različite i nisu incidentne pravoj x i važi $(X,Z_1)\cong(X,Z_2)$ i $(Y,Z_1)\cong(Y,Z_2)$, tada postoji tačka U incidentna pravoj x takva da je $\mathcal{B}(Z_1,U,Z_2)$.

$$\forall X\forall Y\forall Z_1\forall Z_2\forall x\forall\phi\exists U(\mathcal{I}(X,\phi)\wedge\mathcal{I}(Y,\phi)\wedge\mathcal{I}(Z_1,\phi)\wedge\mathcal{I}(Z_2,\phi)\wedge Z_1\neq Z_2$$
$$\mathcal{I}(X,x)\wedge\mathcal{I}(Y,x)\wedge\neg\mathcal{I}(Z_1,x)\wedge\neg\mathcal{I}(Z_2,x)\wedge(X,Z_1)\cong(X,Z_2)\wedge(Y,Z_1)\cong(Y,Z_2)\Rightarrow\mathcal{B}(Z_1,U,Z_2))$$

$\mathcal{P}_3$: $[I8]$ Ako za dve različite ravni postoji jedna tačka koja im je incidentna, onda postoji najmanje još jedna tačka koja im je incidentna.

$$\forall\phi\forall\psi\forall X\exists Y(\phi\neq\psi\wedge\mathcal{I}(X,\phi)\wedge\mathcal{I}(X,\psi)\Rightarrow\mathcal{I}(Y,\phi)\wedge\mathcal{I}(Y,\psi)\wedge X\neq Y)$$

$\mathcal{P}_4$: $[I2]$ Za svake dve različite tačke postoji bar jedna prava kojoj su incidentne.

$$\forall X\forall Y\exists x(X\neq Y\Rightarrow\mathcal{I}(X,x)\wedge\mathcal{I}(Y,x))$$

$\mathcal{P}_5$: $[I5]$ Za svake tri tačke postoji bar jedna ravan kojoj su incidentne.

$$\forall X\forall Y\forall Z\exists\phi(\mathcal{I}(X,\phi)\wedge\mathcal{I}(Y,\phi)\wedge\mathcal{I}(Z,\phi))$$

$\mathcal{P}_6$: $[I1]$ Svakoj pravoj incidentne su najmanje dve različite tačke.

$$\forall x\exists X\exists Y(\mathcal{I}(X,x)\wedge\mathcal{I}(Y,x)\wedge X\neq Y)$$

$\mathcal{P}_7$: $[I4]$ Svakoj ravni incidentne su najmanje tri nekolinearne tačke.

$$\forall\phi\exists X\exists Y\exists Z(\mathcal{I}(X,\phi)\wedge\mathcal{I}(Y,\phi)\wedge\mathcal{I}(Z,\phi)\wedge\neg kolin(X,Y,Z))$$

$\mathcal{P}_8$: [$II4$] Ako su X i Y dve različite tačke, tada postoji tačka Z takva da je $\mathcal{B}(X,Y,Z)$.

$$\forall X \forall Y \exists Z(\mathcal{B}(X,Y,Z))$$

$\mathcal{P}_9$: [$III5$] Ako su X i Y dve različite tačke i tačka Z incidentna nekoj pravoj x, tada postoje tačke U_1 i U_2 incidentne pravoj x takve da važi $(X,Y) \cong (Z,U_1)$, $(X,Y) \cong (Z,U_2)$ i $\mathcal{B}(U_1,Z,U_2)$.

$$\forall X \forall Y \forall Z \forall x \exists U_1 \exists U_2 (X \neq Y \wedge \mathcal{I}(Z,x) \Rightarrow \mathcal{I}(U_1,x) \wedge \mathcal{I}(U_2,x) \wedge (X,Y) \cong (Z,U_1) \wedge (X,Y) \cong (Z,U_2)$$

Jako produktivne aksiome

$\mathcal{JP}_1$: [$I9$] Postoje četiri različite nekoplanarne tačke.

$$\exists X \exists Y \exists Z \exists U (X \neq Y \wedge X \neq Z \wedge X \neq U \wedge Y \neq Z \wedge Y \neq U \wedge Z \neq U \wedge \neg kompl(X,Y,Z,U))$$

Aksioma neprekidnosti[23]

$\mathcal{C}$: Sve rečenice oblika

$$\forall V \forall W \ldots \{\exists Z \forall X Y [\Phi \wedge \Psi \Rightarrow \mathcal{B}(Z,X,Y)] \Rightarrow \exists U \forall x y (\Phi \wedge \Psi \Rightarrow \mathcal{B}(X,U,Y))\}$$

gde je Φ bilo koja formula u kojoj se promenljive $X, V, W, \ldots$, ali ne i Y i Z, pojavljuju kao slobodne, i slično Ψ – sa izmenjenim ulogama za X i Y.

Označićemo sa $\mathcal{E}'$ teoriju koja se dobija kada se u aksiomatskom sistemu teorije $\mathcal{E}$ shema aksioma $\mathcal{C}$ zameni aksiomom $\mathcal{C}'$. Za razliku od teorije $\mathcal{E}$, teorija $\mathcal{E}'$ nije potpuna, ali je konačno aksiomatizovana i pokriva većinu uobičajenih sadržaja koje pokriva teorija $\mathcal{E}$.

$\mathcal{C}'$:

$$\forall X \forall Y \forall Z \forall X_1 \forall Z_1 \forall U \exists Y_1 ((U,X) \cong (U,X_1) \wedge (U,Z) \cong (U,Z_1) \wedge \mathcal{B}(U,X,Z) \wedge \mathcal{B}(X,Y,Z) \Rightarrow$$

$$(U,Y) \cong (U,Y_1) \wedge \mathcal{B}(X_1,Y_1,Z_1))$$

[23] Aksiome $\mathcal{C}$ i $\mathcal{C}'$ preuzete su iz aksiomatskog sistema Tarskog.

Da bi se pojednostavilo izvođenje dokaza, u samom dokazivaču koriste se i sledeće jednostavne teoreme:

Ako je tačka X incidentna pravoj x, onda postoji tačka Y različita od tačke X i incidentna pravoj x.

Ako je tačka X incidentna ravni ϕ, onda postoje tačke Y i Z incidentne ravni ϕ, takve da tačke X, Y i Z nisu kolinearne.

Ako su tačke X i Y različite i incidentne ravni ϕ, onda postoji tačka Z incidentna ravni ϕ, takva da tačke X, Y i Z nisu kolinearne.

Ako postoji tačka X, onda postoje tačke Y, Z i U, takve da tačke X, Y, Z i U nisu komplanarne i svake dve su različite.

Ako postoje različite tačke X i Y, onda postoje tačke Z i U, takve da tačke X, Y, Z i U nisu komplanarne i od te četiri tačke svake dve su različite.

Ako postoje nekolinearne tačke X, Y i Z, onda postoji tačka U, takva da tačke X, Y, Z i U nisu komplanarne i od te četiri tačke svake dve su različite.

Ako važi $kolin(X,Y,Z)$, onda važi i $kolin(X,Z,Y)$, $kolin(Y,X,Z)$, $kolin(Y,Z,X)$, $kolin(Z,X,Y)$ i $kolin(Z,Y,X)$

Ako važi $kompl(X,Y,Z,U)$, onda važi i $kompl(X,Y,U,Z)$, $kompl(X,Z,Y,U)$, $kompl(X,Z,U,Y)$, $kompl(X,U,Y,Z)$, $kompl(X,U,Z,Y)$, $kompl(Y,X,Z,U)$, $kompl(Y,X,U,Z)$, $kompl(Y,Z,X,U)$, $kompl(Y,Z,U,X)$, $kompl(Y,U,X,Z)$, $kompl(Y,U,Z,X)$, $kompl(Z,X,Y,U)$, $kompl(Z,X,U,Y)$, $kompl(Z,Y,X,Z)$, $kompl(Z,Y,Z,X)$, $kompl(Z,U,X,Y)$, $kompl(Z,U,Y,X)$, $kompl(U,X,Y,Z)$, $kompl(U,X,Z,Y)$, $kompl(U,Y,X,Z)$, $kompl(U,Y,Z,X)$, $kompl(U,Z,X,Y)$ *i* $kompl(U,Z,Y,X)$.

Ako su različite tačke X, Y i Z i prava x takve da su tačke X i Y incidentne pravoj x, a tačka Z nije, onda tačke X, Y i Z nisu kolinearne .

Ako su tačke X, Y, Z i V, od kojih su svake tri nekolinearne, i ravan ϕ takve da su tačke X, Y, Z incidentne ravni ϕ, a tačka V nije, onda tačke X, Y, Z i V nisu komplanarne .

Ako su tačke X, Y i Z kolinearne, i ako su tačke X i Y različite i incidentne su pravoj x, onda je pravoj x incidentna i tačka Z.

Ako su tačke X, Y, Z i U komplanarne, i ako su tačke X, Y i Z nekolinearne i incidentne su ravni ϕ, onda je ravni ϕ incidentna i tačka U.

Za svake tri tačke X, Y i Z, ako važi $B(X,Y,ZC)$, onda ne važi $(X,Y) \cong (X,Z)$.

Za svaku pravu x, svaku tačku X i svaku ravan ϕ takve da je tačka X incidentna ravni ϕ, a nije incidentna pravoj x i da je prava x incidentna ravni ϕ, postoji prava incidentna ravni ϕ takva da joj je incidentna tačka X, a ne seče se sa pravom x.

1.4.2 Klasifikacija i struktura aksioma

Primetimo da, izuzev aksiome neprekidnosti $\mathcal{C}$, sve aksiome teorije $\mathcal{E}$, uključujući aksiome zasnovanosti i aksiome jednakosti, kao i aksioma $\mathcal{C}'$, imaju jednu od sledećih formi:

$$\forall x_1 \forall x_2 \ldots \forall x_n \exists y_1 \exists y_2 \ldots \exists y_m (\Phi(x_1, x_2, ..., x_n) \Rightarrow \Psi(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m)) \quad (n, m \geq 1) \tag{1.1}$$

$$\begin{aligned} &\forall x_1 \forall x_2 \ldots \forall x_n \exists y_1 \exists y_2 \ldots \exists y_m (\Phi(x_1, x_2, ..., x_n) \Rightarrow \\ &\Psi_1(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m) \vee \Psi_2(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m) \vee \ldots \\ &\ldots \vee \Psi_k(x_1, x_2, \ldots x_n, y_1, y_2, \ldots y_m)) \quad (n, m \geq 1) \end{aligned} \tag{1.2}$$

$$\forall x_1 \forall x_2 \ldots \forall x_n (\Phi(x_1, x_2, ..., x_n) \Rightarrow \Psi(x_1, x_2, ..., x_n)) \quad (n \geq 1) \tag{1.3}$$

$$\exists y_1 \exists y_2 \ldots \exists y_m (\Psi(y_1, y_2, ..., y_m)) \quad (m \geq 1) \tag{1.4}$$

gde su Φ, Ψ i Ψ_i literali nad nekim od promenljivih $x_1, x_2, ..., x_n$, odnosno $y_1, y_2, ..., y_m$.

Jednu od navedenih formi ima i svaka od definicija i teorema navedenih u poglavlju 1.4.1. U dokazivaču EUKLID koristimo i njih na sličan (ili isti) način kao aksiome.

Prvu od navedenih formi zvaćemo *univerzalno-egzistencijalnom* (formom $\exists\forall$), drugu *univerzalno-egzistencijalno-disjunktnom* (formom $\exists\forall\vee$), treću *univerzalnom* (formom $\forall$) i četvrtu *egzistencijalnom* (formom $\exists$) [24]. Sve četiri forme označavaćemo zajedno sa $\mathcal{F}$.

Strukturom aksioma i efikasnošću izvođenja dokaza i prirodom dokazivača EUKLID motivisana je nova klasifikacija geometrijskih aksioma. Po toj klasifikaciji, geometrijske aksiome ne delimo (kao što je uobičajeno) na aksiome incidencije, rasporeda, podudarnosti, neprekidnosti i paralelnosti - ne delimo ih po "temi" o kojoj govore, već po njihovoj strukturi i to na:

-*logičke* aksiome (aksiome zasnovanosti i aksiome jednakosti);
-*neproduktivne* aksiome (univerzalne aksiome);
-*granajuće* aksiome (univerzalno-egzistencijalno-disjunktne aksiome);
-*produktivne* aksiome (univerzalno-egzistencijalne aksiome);
-*jako produktivne*[25] aksiome (egzistencijalne aksiome);

Navedena podela aksioma, koja je proistekla iz samog koncepta dokazivača prirodno odgovara formama struktura aksioma o kojima je već bilo reči. Po kriterijumima po kojima su

[24] O ovakvim formama geometrijskih aksioma pisao je i Tarski (v. [Ta71, str.171]), ali u drugom kontekstu.

[25] U jednoj verziji dokazivača EUKLID, zbog veće efikasnosti izvođenja dokaza, neke od produktivnih aksioma (one koje zahtevaju "slabe" uslove) svrstane su među jako produktivne i celoj grupi dat je poseban status. Time je smanjena "produkcija" novih objekata i samim tim povećana efikasnot izvođenja dokaza. Ipak, upravo zbog promenjenih kriterijuma za uvođenje novih objekata, ta verzija dokazivača ne može da izvede sve dokaze koje može osnovna verzija.

razvrstane u grupe, aksiome su poređane i okviru grupa. Taj poredak nije utvrđen potpuno egzaktno, već u skladu sa intuitivnim ocenama stepena u kojem se ispoljava svojstvo odgovarajuće grupe aksioma, ali i u skladu sa brojnim eksperimentima i potvrđenim primerima "efikasnih" dokaza. Raspored aksioma u okviru grupa važan je zbog efikasnosti izvođenja dokaza, ali ne utiče na skup teorema koje dokazivač EUKLID može da dokaže.

1.4.3 Svojstva teorije $\mathcal{E}$

U ovom delu teksta, smatrajući (za sada) da koristimo neki od uobičajenih sistema izvođenja, utvrdićemo svojstva teorije $\mathcal{E}$[26]. Pre toga, definisaćemo interpretaciju teorije $\mathcal{E}$ u nekom modelu $\mathcal{F}$ teorije realno zatvorenog polja.

Neka je sistem $\mathcal{F} = (F, -, \cdot, \leq)$ uređeno polje (F je skup, $+$ i $\cdot$ su binarne operacije za koje je F zatvoren i $\leq$ je binarna relacija nad elementima iz F). Kažemo da je uređeno polje $\mathcal{F}$ *euklidsko* ako je svaki nenegativni element skupa F kvadrat (tj. ako važi $\forall x \exists y (0 \leq x \Rightarrow x = y \cdot y)$). Kažemo da je uređeno polje $\mathcal{F}$ *realno zatvoreno* ako je euklidsko i ako svaki polinom neparnog stepena sa koeficijentima u F, ima nulu u F.

Neka je $F^3 = F \times F \times F$ skup svih trojki (x, y, z) $(x, y, z \in F)$. Podskupove A_0, A_1 i A_2 skupa $\mathcal{P}(F^3)$ ($\mathcal{P}(F^3)$ je partitivni skup skupa F^3) definišemo na sledeći način:

$$a \in A_0 \text{ ako i samo ako } a = \{(x, y, z)\}$$

$$a \in A_1 \text{ ako i samo ako } \exists x_0 \exists y_0 \exists z_0 \exists f_1 \exists f_2 \exists f_3 \forall x \forall y \forall z ((x, y, z) \in a \Leftrightarrow f_2(x - x_0) = f_1(y - y_0), f_3(x - x_0) = f_1(z - z_0))$$

$$a \in A_2 \text{ ako i samo ako } \exists f_1 \exists f_2 \exists f_3 \exists f_4 \forall x \forall y \forall z ((x, y, z) \in a \Leftrightarrow f_1 x + f_2 y + f_3 z + f_4 = 0$$

Neka je $A_{\mathcal{F}} = A_0 \cup A_1 \cup A_2$. Predikatske simbole $\mathcal{S}$, $\mathcal{L}$, $\mathcal{P}$, $=$, $\mathcal{B}$ i $\cong$ preslikavamo (interpretacijom I) u relacije $\mathcal{S}_{\mathcal{F}}$, $\mathcal{L}_{\mathcal{F}}$, $\mathcal{P}_{\mathcal{F}}$, $=_{\mathcal{F}}$, $\mathcal{I}_{\mathcal{F}}$, $B_{\mathcal{F}}$ i $D_{\mathcal{F}}$ nad elementima iz $A_{\mathcal{F}}$ definisane na sledeći način:

$$\mathcal{S}_{\mathcal{F}}(a) \text{ ako i samo ako } a \in A_0$$

$$\mathcal{L}_{\mathcal{F}}(a) \text{ ako i samo ako } a \in A_1$$

$$\mathcal{P}_{\mathcal{F}}(a) \text{ ako i samo ako } a \in A_2$$

$$a =_{\mathcal{F}} b \text{ ako i samo ako } a = b$$

[26] Teoreme 1.2 – 1.7 zasnovane su na rezultatima i idejama iz teksta *What is Elementary Geometry ?* Alfreda Tarskog koje se odnose na geometrijski sistem uveden u tom tekstu (v.[Ta71]).

$\mathcal{I}_{\mathcal{F}}(a,b)$ ako i samo ako $a \subset b$

$B_{\mathcal{F}}(a,b,c)$ ako i samo ako

$$a=\{(x_a,y_a,z_a)\}, b=\{(x_b,y_b,z_b)\}, c=\{(x_c,y_c,z_c)\}, \neg(a=b), \neg(b=c),$$
$$(x_a-x_b)(y_b-y_c)=(x_b-x_c)(y_a-y_b), (x_a-x_b)(z_b-z_c)=(x_b-x_c)(z_a-z_b),$$
$$0\leq(x_a-x_b)(x_b-x_c), 0\leq(y_a-y_b)(y_b-y_c), 0\leq(z_a-z_b)(z_b-z_c)$$

$(a,b)\cong_{\mathcal{F}}(c,d)$ ako i samo ako

$$a=\{(x_a,y_a,z_a)\}, b=\{(x_b,y_b,z_b)\}, c=\{(x_c,y_c,z_c)\}, d=\{(x_d,y_d,z_d)\},$$
$$(x_a-x_b)^2+(y_a-y_b)^2+(z_a-z_b)^2=(x_c-x_d)^2+(y_c-y_d)^2+(z_c-z_d)^2$$

Teorema 1.1 : $\mathcal{D}(\mathbf{R})=(A_{\mathbf{R}},I)$ je model teorije $\mathcal{E}$[27]

Dokaz:
Sve aksiome teorije $\mathcal{E}$ tačne su u modelu $\mathcal{D}(\mathbf{R})$. Kao ilustraciju, dokazaćemo tvrđenje za nekoliko aksioma.

Aksioma $\mathcal{P}_5$
Neka su $a=\{(x_a,y_a,z_a)\}$ i $b=\{(x_b,y_b,z_b)\}$ dve proizvoljne različite tačke $(\mathcal{S}_{\mathbf{R}}(a),\mathcal{S}_{\mathbf{R}}(b))$. Postoji prava p $(\mathcal{L}_{\mathbf{R}}(p))$ takva da je

$$(x,y,z)\in p\Leftrightarrow(y_b-y_a)(x-x_a)=(x_b-x_a)(y-y_0),\ (z_b-z_a)(x-x_a)=(x_b-x_a)(z-z_0).$$

Važi $a\subset p$ i $b\subset p$, tj. $\mathcal{I}_{\mathbf{R}}(a,p)$ i $\mathcal{I}_{\mathbf{R}}(b,p)$, što je i trebalo dokazati.

Aksioma $\mathcal{N}_9$
Neka su $a=\{(x_a,y_a,z_a)\}$ i $b=\{(x_b,y_b,z_b)\}$ dve proizvoljne tačke $(\mathcal{S}_{\mathbf{R}}(a),\mathcal{S}_{\mathbf{R}}(b))$. Tada je

$$(x_a-x_b)^2+(y_a-y_b)^2+(z_a-z_b)^2=(x_b-x_a)^2+(y_b-y_a)^2+(z_b-z_a)^2$$

tj. $(a,b)\cong_{\mathbf{R}}(b,a)$, što je i trebalo dokazati.

Aksioma $\mathcal{P}_8$
Neka su $a=\{(x_a,y_a,z_a)\}$ i $b=\{(x_b,y_b,z_b)\}$ dve proizvoljne različite tačke $(\mathcal{S}_{\mathbf{R}}(a),\mathcal{S}_{\mathbf{R}}(b))$. Postoji tačka c $(\mathcal{S}_{\mathbf{R}}(c))$ takva da je

$$c=\{(x_c,y_c,z_c)\},\quad\text{gde je}\quad x_c=2x_b-x_a,\ y_c=2y_b-y_a,\ z_c=2z_b-z_a.$$

[27] $\mathbf{R}$ je uređeno polje realnih brojeva.

Neposredno se proverava da za tako odabranu tačku c važi $B_{\mathbf{R}}(a,b,c)$.

Teorema 1.2 : $\mathcal{M}$ je model teorije $\mathcal{E}$ ako i samo ako je $\mathcal{M}$ izomorfan sa modelom $\mathcal{D}(\mathcal{F})$ nad nekim realno zatorenim poljem $\mathcal{F}$.

Dokaz:

($\Leftarrow$:) Na osnovu teoreme 1.1 $\mathcal{D}(\mathbf{R})$ je model teorije $\mathcal{E}$. Svako realno zatvoreno polje $\mathcal{F}$ je elementarno ekvivalentno sa poljem $\mathbf{R}$ (tj. svaka rečenica koja važi u jednom polju važi u drugom i obratno) (v. [Ta51]). Iz toga sledi da je model $\mathcal{D}(\mathcal{F})$ nad poljem $\mathcal{F}$ elementarno ekvivalentan sa $\mathcal{D}(\mathbf{R})$, pa je $\mathcal{D}(\mathcal{F})$ model teorije $\mathcal{E}$. Iz toga proizilazi da je svaki sistem $\mathcal{M}$ koji je izomorfan sa $\mathcal{D}(\mathcal{F})$ takođe model teorije $\mathcal{E}$.

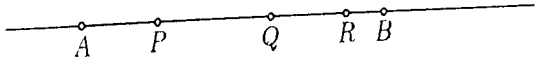
$$\begin{array}{ccc} \mathcal{D}(\mathbf{R}) & \equiv & \mathcal{D}(\mathcal{F}) \\ \approx & & \models \\ \mathcal{M} & \models & \mathcal{E} \end{array}$$

($\Rightarrow$:) Neka je $\mathcal{M}$ model teorije $\mathcal{E}$. (Zbog jednostavnosti, tačke u modelu $\mathcal{M}$ označavaćemo velikim, prave malim latiničnim slovima, a ravni slovima grčkog alfabeta.) Na osnovu aksiome $\mathcal{IP}_1$ postoje četiri različite nekomplanarne tačke A, B, C i D.

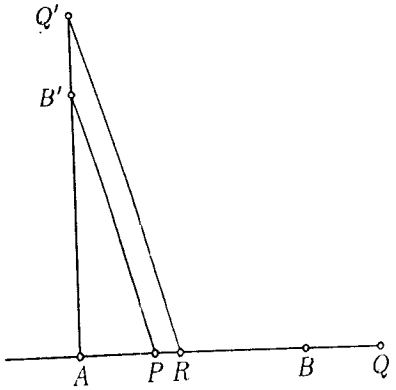
Na osnovu aksiome $\mathcal{P}_4$ postoji prava kojoj su incidentnte tačke A i B (neka je to prava a_1). Na osnovu aksiome $\mathcal{P}_5$ postoji ravan kojoj su incidentne tačke A, B i C (označimo je sa π_1). Može se dokazati da postoji jedinstvena prava (označimo je sa a_2) takva da je upravna na pravoj a_1, da je incidentna ravni π_1 i da joj je incidentna tačka A (za definiciju upravnosti i dokaz pomenutog tvrđenja videti npr. [Lu94,str.94] (analogno bi bili formulisani i za teoriju $\mathcal{E}$)). Može se dokazati da postoji jedinstvena prava (označimo je sa a_3) takva da je upravna na ravni π_1 i da joj je incidentna tačka A (za definiciju upravnosti prave i ravni i dokaz pomenutog tvrđenja videti npr. [Lu94,str.97] (analogno bi bili formulisani i za teoriju $\mathcal{E}$)). Neka su B_2 i B_3 tačke različite od tačke A i incidentne redom pravama a_2 i a_3. Neka je π_2 ravan kojoj su incidentne prave a_1 i a_3, a π_3 ravan kojoj su incidentne prave a_2 i a_3.

Neka je F skup svih tačaka koje su incidentne pravoj a_1. Definišimo relaciju $\leq$ za sve parove tačaka incidentnih pravoj a_1. Ako su tačke P i Q tačke incidentne pravoj a_1 kažemo da je $P \leq Q$ ako su tačke P i Q identične ili ako je $\mathcal{B}(P,A,B)$ i nije $\mathcal{B}(Q,P,A)$ ili ako je $\mathcal{B}(A,P,Q)$ i nije $\mathcal{B}(P,A,B)$.

Definišimo operaciju $+$ za sve parove tačaka incidentnih pravoj a_1. Ako su tačke P i Q tačke incidentne pravoj a_1, paru tačaka (P,Q) pridružujemo tačku R (pišemo $P+Q=R$) takvu da je $(A,P) \cong (Q,R)$ i važi $A \leq P$ i $Q \leq R$ ili važi $P \leq A$ i $R \leq Q$.



slika 1.1



slika 1.2

Definišimo operaciju $\cdot$ za sve parove tačaka incidentnih pravoj a_1. Ako su tačke P i Q tačke incidentne pravoj a_1 paru tačaka (P,Q) (pretpostavimo da važi $A \leq P$ i $A \leq Q$) pridružujemo tačku R (pišemo $P \cdot Q = R$) izabranu na sledeći način: neka je B' tačka incidentna pravoj a_2 takva da je $(A,B) \cong (A,B')$; neka je Q' tačka incidentna pravoj a_2 takva da je $(A,Q) \cong (A,Q')$ i nije $\mathcal{B}(B',A,Q')$; neka je p prava kojoj su incidentne tačke P i B'; tačka B' nije incidentna pravoj a_1, pa prave a_1 i p nisu identične; neka je q prava incidentna ravni π takva da joj je incidentna tačka Q' i takva da je paralelna pravoj p (za definiciju paralelnosti i dokaz da pomenuta prava q postoji videti npr. [Lu94, str.193] (analogno bi bili formulisani i za teoriju $\mathcal{E}$)); neka je R incidentna pravoj a_1 i pravoj q (takva tačka postoji; zaista, ako se prave a_1 i q ne bi sekle, to bi značilo da u ravni π_1 postoje dve različite prave (a_1 i p) kojima je incidentna tačka P i koje su paralelne pravoj q, što je kontradiktorno sa tvrđenjem koje se može dokazati u teoriji $\mathcal{E}$ (za analogni dokaz videti npr. [Lu94,str.204])). Slično definišemo operaciju $\cdot$ i ako ne važi $A \leq P$ i $A \leq Q$.

Korišćenjem aksioma sistema $\mathcal{E}$ bez aksiome neprekidnosti može se dokazati da je sistem $\mathcal{F} = (F,+,\cdot,\leq)$ uređeno polje, a korišćenjem i aksiome neprekidnosti može se dokazati da je sistem $\mathcal{F}$ realno zatvoreno polje.

Neka je T proizvoljna tačka i neka su T_1, T' i T'' podnožja upravnih iz tačke t na pravama a_1, a_2 i a_3. Neka je x_2 tačka incidentna pravoj a_1 takva da je $(A,y_T) \cong (A,T_2)$ i $\mathcal{B}(T_2,A,B)$ (ukoliko je $\mathcal{B}(T',A,B_2)$) odnosno $\neg\mathcal{B}(T_2,A,B)$ (ukoliko je $\neg\mathcal{B}(T',A,B_2)$).

Neka je T_3 tačka incidentna pravoj a_1 takva da je $(A,T'') \cong (A,T_3)$ i $\mathcal{B}(T_3,A,B)$ (ukoliko je $\mathcal{B}(T'',A,B_3)$) odnosno $\neg\mathcal{B}(T_3,A,B)$ (ukoliko je $\neg\mathcal{B}(T'',A,B_3)$).

Tački T pridružujemo trojku $\hat{t} = (T_1,T_2,T_3)$, tj. trojku elemenata realno zatvorenog polja $\mathcal{F}$. Ta trojka je jedinstveno određena, i obratno, svakoj trojki odgovara jedinstveno određena tačka. Pravoj p pridružujemo skup $\hat{p}$ svih trojki pridruženih tačkama koje su incidentne pravoj p. Ravni r pridružujemo skup $\hat{r}$ svih trojki pridruženih tačkama koje su incidentne ravni p.

Može se dokazati da važi

$$\mathcal{S}(a) \text{ ako i samo ako } \mathcal{S}_{\mathcal{F}}(\hat{a}),$$
$$\mathcal{L}(a) \text{ ako i samo ako } \mathcal{L}_{\mathcal{F}}(\hat{a}),$$
$$\mathcal{P}(a) \text{ ako i samo ako } \mathcal{P}_{\mathcal{F}}(\hat{a}),$$
$$a = b \text{ ako i samo ako } \hat{a} =_{\mathcal{F}} \hat{b},$$
$$\mathcal{I}(a,b) \text{ ako i samo ako } \mathcal{I}_{\mathcal{F}}(\hat{a},\hat{b}),$$
$$\mathcal{B}(a,b,c) \text{ ako i samo ako } B_{\mathcal{F}}(\hat{a},\hat{b},\hat{c}) \text{ i}$$
$$(a,b) \cong (c,d) \text{ ako i samo ako } (\hat{a},\hat{b}) \cong_{\mathcal{F}} (\hat{c},\hat{d}),$$

iz čega sledi da su sistemi $\mathcal{M}$ i $\mathcal{D}(\mathcal{F})$ izomorfni, što je i trebalo dokazati.

Posledica: Rečenica teorije $\mathcal{E}$ je teorema ako i samo ako je tačna u modelu $\mathcal{D}(\mathbf{R})$.

Dokaz:

($\Rightarrow$:) Na osnovu teoreme **1.1**, $\mathcal{D}(\mathbf{R})$ je model teorije $\mathcal{E}$, pa je svaka teorema teorije $\mathcal{E}$ tačna u $\mathcal{D}(\mathbf{R})$.

$\Leftarrow$:) Na osnovu teoreme **1.2**, sistem $\mathcal{D}(\mathbf{R})$ elementarno je ekvivalentan svakom modelu teorije $\mathcal{E}$, pa ukoliko je neka rečenica tačna u $\mathcal{D}(\mathbf{R})$, onda je ona tačna u svakom modelu teorije $\mathcal{E}$, iz čega proizilazi da je ona teorema teorije $\mathcal{E}$.

Teorema 1.3 : Teorija $\mathcal{E}$ je potpuna i neprotivrečna.

Dokaz:

Ako za neku teoriju $\mathcal{T}$ postoji model $\mathcal{M}$ takav da je rečenica teorema teorije $\mathcal{T}$ ako i samo ako je ona tačna u modelu $\mathcal{M}$, onda je ta teorija neprotivrečna i potpuna. Dakle, na osnovu posledice teoreme **1.2** neposredno sledi da je teorija $\mathcal{E}$ neprotivrečna i potpuna.

Svojstvo potpunosti može se dokazati i na drugi način. Naime, teorija je potpuna ako za svaku njenu rečenicu važi da je tačna u svakom modelu ili u nijednom modelu teorije, odnosno ako su svaka dva modela elementarno ekvivalntna. Zaista, ako je neka rečenica teorije $\mathcal{E}$ tačna u modelu $\mathcal{M}_1$, onda je ona tačna i u modelu $\mathcal{D}(\mathbf{R})$ (jer su oni elementarno ekvivalentni). Slično, ako je rečenica tačna u $\mathcal{D}(\mathbf{R})$, onda je ona tačna i u svakom modelu $\mathcal{M}_2$ teorije $\mathcal{E}$ (jer su oni elementarno ekvivalentni). Dakle, neka rečenica je tačna u modelu $\mathcal{M}_1$ ako i samo ako je tačna u modelu $\mathcal{M}_2$, pa su svaka dva modela teorije $\mathcal{E}$ elementarno ekvivalentna, iz čega proizilazi da je teorija $\mathcal{E}$ potpuna.

Teorema 1.4 : Teorija $\mathcal{E}$ je odlučiva.

Dokaz:

Na osnovu poznate teoreme (v. [Ta71,str.14]) potpuna teorija sa standardnom formalizacijom (tj. teorija koje može biti zasnovana u okviru predikatskog računa prvog reda sa jednakošću) i sa rekurzivnim skupom aksioma je odlučiva. Teorija $\mathcal{E}$ je teorija sa standarnom

formalizacijom, sa rekurzivnim (iako beskonačnim) skupom aksioma i pri tom je, na osnovu teoreme **1.3**, potpuna, pa je odlučiva.

Teorema 1.5 : Teorija $\mathcal{E}$ ne može biti konačno aksiomatizovana.

Dokaz:
Korišćenjem aksioma sistema $\mathcal{E}$ bez aksioma neprekidnosti može se dokazati da je sistem $\mathcal{F} = (F, +, \cdot, \leq)$ konstruisan u okviru dokaza teoreme **1.2** uređeno polje. Beskonačna shema aksioma neprekidnosti može biti zamenjena prebrojivim skupom aksioma (tako da su stara i nova teorija ekvivalentne): $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \ldots$ gde $\mathcal{S}_0$ predstavlja tvrđenje da je polje $\mathcal{F}$ euklidsko, a aksioma $\mathcal{S}_n$ $(n > 0)$ predstavlja tvrđenje da u polju $\mathcal{F}$ svaki polinom stepena $2n + 1$ ima nulu. Za svaki prost broj p može se konstruisati uređeno polje $\mathcal{F}_p$ u kojem svaki polinom stepena $2n + 1 < p$ ima nulu i pri tom postoji polinom stepena p koji nema nulu. Dakle, postoji sistem $(\mathcal{D}(\mathcal{F}_p))$ (p je prost broj) u kojem su zadovoljene sve aksiome teorije $\mathcal{E}$ bez aksioma neprekidnosti i aksiome $\mathcal{S}_n$, za $n < m$ $(2m + 1 = p)$, ali ne i aksioma $\mathcal{S}_m$. To znači da aksiomatski sistem koji čine geometrijske aksiome bez neprekidnosti i skup aksioma $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \ldots$ ne može biti zamenjen ekvivalentnim konačnim skupom aksioma i dalje, da teorija $\mathcal{E}$ ne može biti konačno aksiomatizovana.

Teorija $\mathcal{E}$, dakle, ne može biti konačno aksiomatizovana, ali se među njenim podteorijama izdvaja (konačno aksiomatizovana) $\mathcal{E}'$, u okviru koje je moguće dokazati mnoštvo teorema teorije $\mathcal{E}$ (većinu onih iz uobičajenih kurseva geometrije). Između ostalih teorema teorije $\mathcal{E}$ koje ne važe u $\mathcal{E}'$ su teoreme koje ne mogu biti dokazane korišćenjem tzv. elementarnih konstrukcija (pomoću lenjira i šestara) kao što je npr. teorema koja tvrdi da za svaki ugao postoje dve poluprave koje ga razlažu na tri podudarna ugla.

Teorema 1.6 : $\mathcal{M}$ je model teorije $\mathcal{E}'$ ako i samo ako je $\mathcal{M}$ izomorfan sa modelom $\mathcal{D}(\mathcal{F})$ nad nekim euklidskim poljem $\mathcal{F}$.

Navedena teorema može biti dokazana na sličan način kao teorema **1.2**. Kako postoje euklidska polja koja su realno zatvorena i ona koja to nisu, važi sledi tvrđenje:

Teorema 1.7 : Teorija $\mathcal{E}'$ je nepotpuna.

U tekstu *What is elementary geometry ?* Alfred Tarski (v. [Ta71, str.174]) je za tamo izložen geometrijski aksiomatski sistem (analogan sistemu $\mathcal{E}$) izneo je i hipotezu koja može biti formulisana i za teoriju $\mathcal{E}'$:

Hipoteza Tarskog 1: Teorija $\mathcal{E}'$ nije odlučiva.

Pored pomenute hipoteze, Tarski je u istom tekstu postavio i hipotezu da važi još jače tvrđenje koje analogno može biti formulisano za teoriju $\mathcal{E}$:

Hipoteza Tarskog 2: Bilo koja konačno aksiomatizovana podteorija teorije $\mathcal{E}$ nije odlučiva.

2

DEDUKCIJA

2.1 Razvoj sistema za izvođenje dokaza

Vekovima je izvođenje dokaza bilo zasnivano isključivo na sistemu aristotelovskih silogizama. Verovatno prvi nagoveštaj predikatskog računa i pravila izvođenja kakve danas poznajemo nalazimo u tekstovima Lajbnica, u kojima on nagoveštava svoj veliki projekat – razvoj "računa zaključivanja" (lat. *calculus ratiocanator*) i "univerzalnog jezika" (lat. *lingua characteristica*). Gledajući daleko ispred svog vremena, on za svoj planirani sistem govori "... da će biti oslobođen nužnosti razmišljanja o stvarima samim, ali ipak će sve biti ispravno". Na žalost, u svom ambicioznom projektu koji je trebalo da se odnosi na sve nauke, Lajbnic nije otišao mnogo dalje od Aristotelovog sistema i razvio je tek mali deo onog što danas zovemo Bulovom algebrom. Tek dva veka nakon pojavljivanja pomenutih Labnicovih ideja, definisan je prvi "račun zaključivanja" (Džordž Bul, 1847), a dvadesetak godina nakon toga napravljen je i prvi mehanički sistem koji ga je koristio – mašina za proveravanje bulovskih identiteta koju je 1869. konstruisao Stenli Dževons. Ključni rad u definisanju danas uobičajenog predikatskog računa, verovatno je *Begriffsschrift* (*"zapisivanje koncepata"*) Gotliba Fregea iz 1879. godine u kojem su, između ostalog, precizno uvedeni fomalni jezik i svojstva kvantifikatora i u kojem je ključno mesto u izvođenju dokaza dato pravilu *modus ponens*. Ovaj rad može se smatrati i direktnim začetnikom moderne logike i formalnih jezika (uključujući i programske jezike). Nakon toga, sledile su decenije burnog razvoja logike ispunjene značajnim rezultatima i oštrim raspravama i suprotstavljanjima po pitanjima poimanja formalnih jezika, dokaza, beskonačnosti i posebno koncepta intuicionističke matematike (u to vreme oličenog pre svih u Braueru). U odbranu klasične matematike od napada intuicionista (koji prihvataju samo konstruktivne metode u izvođenju dokaza) formulisani su jasni "metamatematički programi" u jednom radu Emila Posta iz 1920. godine (koji se odnosio na iskazni račun) i 1928. godine u znamenitoj knjizi *Grundzuge der Theoretischen Logik* Hilberta i Akermana. U ovoj knjizi formulisana je aksiomatika za predikatski račun i dokazano mnoštvo njegovih svojstava (između ostalog i svojstvo potpunosti). Ostao je otvoren tzv. *Entscheidungsproblem* – problem pronalaženja opšteg algoritma koji za datu rečenicu proverava da li je teorema. Negativan odgovor na ovaj problem stigao je nekoliko godina kasnije u rezultatima Gedela,

Skolema i Tjuringa u kojima je dokazano postojanje (esencijano) nepotpunih i neodlučivih teorija (v.npr.[Men64],[Ta69] ili [Mi86]).

Već od tog vremena – od prve četvrtine XX veka, istorija razvoja teorije dokaza gotovo se poklapa sa istorijom razvoja automatskog dokazivanja teorema. Radovi Skolema i Herbranda iz dvadesetih i tridesetih godina bili su od presudnog uticaja na veliku većinu sistema za automatsko dokazivanje teorema (zasnovanih na prikladnim pravilima izvođenja). To se pogotovu odnosi na šezdesete i sedamdesete godine kada oblast automatske dedukcije uzima maha i kada su razvijeni mnogi značajni sistemi izvođenja prilagođeni automatskoj primeni – pomenimo samo metod tabloa (Evert Bet, 1958.) i, jedno vreme dominantan, metod rezolucije (Alen Robinson, 1963.). Uprkos kociznosti metoda rezolucije koja se ogledala u primeni samo jednog pravila izvođenja i uprkos ogromnoj energiji uloženoj u unapređenja, velika početna očekivanja počela su da splašnjavaju (najpre pod uticajem istraživača sa MIT-a) i sve se manje verovalo da metod rezolucije, bez obzira na modifikacije, može da dovede do efikasnih rešenja u automatskom dokazivanju teorema. Već sedamdesetih godina istraživači se okreću kvalitativno drugačijim pristupima, tragajući sve češće za mogućnostima za formalizaciju i oponašanje uobičajenog, intuitivnog rasuđivanja. Teorijsku bazu za takve sisteme često predstavlja prirodna dedukcija – sistem koji je tridesetih i četrdesetih godina razvio Gerhard Gencen (v. dodatak i [Gen, str 68], [Pr65]) sa početnom motivacijom koju oslikavaju sledeće rečenice: "... formalizacija logičke dedukcije, pogotovu kako su je razvili Frege, Rasel i Hilbert, prilično je daleko od formi dedukcije koje se u praksi koriste u matematičkim dokazima. Zauzvrat su dobijene značajne formalne prednosti. Suprotno, ja sam odlučio da izgradim formalni sistem koji je, koliko je to moguće, blizak stvarnom rasuđivanju. Rezultat je 'račun prirodne dedukcije' (NJ za intuicionističku i NK za klasičnu predikatsku logiku) ...". Na tragu Gencenovih radova razvijeno je više njegovih varijanti i sistema za automatsko dokazivanje teorema.

2.2 Sistem izvođenja dokaza u dokazivaču EUKLID

U izgradnji sistema EUKLID, težilo se ka formulisanju i primeni pravila izvođenja (u okvirima predikatskog računa prvog reda) koja su uobičajena u geometriji, kako bi generisani dokazi bili što bliži tradicionalnim, intuitivnim dokazima. S druge strane, sistemu pravila izvođenja morala se obezbediti prezicnost, a redudancija svesti na što manju meru. Sistem izvođenja koji se koristi u dokazivaču EUKLID je "negde između" Gencenovog i Hilbertovog koncepta i ima ograničenje da može da se koristi samo sa dokazivanje tereoma jedne klase zapisanih u konkretnoj formi (pri čemu, u nekom od uobičajenih sistema (v.npr.[Men64,str 57]), može da se dokaže da je svaku teoremu te klase moguće zapisati u toj, specifičnoj formi). Jedno od svojstava formulisanog sistema je (slično kao i u Gencenovom sistemu) da se intuicionistička i klasična varijanta razlikuju u samo jednoj aksiomi (u aksiomi *tertium non datur*).

Usvojimo najpre dogovor po kojem ćemo rečenice oblika

$$\forall x_1 \forall x_2 \ldots \forall x_n \exists y_1 \exists y_2 \ldots \exists y_m \Theta(x_1, x_2, \ldots x_n, y_1, y_2, \ldots y_m)$$

zapisivati kraće kao

$$\forall \vec{x} \exists \vec{y} \Theta(\vec{x}, \vec{y})$$

U dokazivaču EUKLID dokazujemo teoreme teorije $\mathcal{E}'$ koje imaju jednu od sledećih formi:

$$\forall\vec{x}\exists\vec{y}\Theta(\vec{x},\vec{y})$$

$$\forall\vec{x}\Theta(\vec{x})$$

$$\exists\vec{y}\Theta(\vec{y})$$

(Θ označava formulu teorije $\mathcal{E}'$ bez kvantifikatora i bez slobodnih promenljivih).

Primetimo da sve aksiome teorije $\mathcal{E}'$ imaju jednu od navedenih formi, tj. da su forme $\mathcal{F}$ (v. poglavlje 1.4.2) specijalni slučajevi gore navedenih formi.

2.2.1 Shema dokaza u dokazivaču EUKLID

Pretpostavimo da treba dokazati teoremu oblika

$$\forall\vec{x}\exists\vec{y}\Theta(\vec{x},\vec{y})$$

(Θ označava formulu teorije $\mathcal{E}'$ bez kvantifikatora i bez slobodnih promenljivih). Formula $\Theta(\vec{x},\vec{y})$ može se napisati u disjunktivnoj normalnoj formi (v.[Men64,str.25]):

$$\Theta(\vec{x},\vec{y}) \equiv \Theta_1(\vec{x},\vec{y}) \vee \Theta_2(\vec{x},\vec{y}) \vee \ldots \vee \Theta_p(\vec{x},\vec{y}) \tag{2.1}$$

(Θ_i su konjunkcije literala).

Ako su formule $\Theta_1, \Theta_2, \ldots \Theta_k$ $(k > 0)$ literali (samo) nad promenljivim $\vec{x}$, onda je:

$$\Theta(\vec{x},\vec{y}) \equiv \Theta_1(\vec{x}) \vee \ldots \vee \Theta_k(\vec{x}) \vee \Theta_{k+1}(\vec{x},\vec{y}) \ldots \vee \Theta_p(\vec{x},\vec{y})$$

$$\Theta(\vec{x},\vec{y}) \equiv \neg(\neg\Theta_1(\vec{x}) \wedge \ldots \wedge \neg\Theta_k(\vec{x})) \vee \Theta_{k+1}(\vec{x},\vec{y}) \ldots \vee \Theta_p(\vec{x},\vec{y})$$

Ako je formula $\Theta_i(\vec{x})$ $(1 \leq i \leq k)$ atomička, neka je $\Phi_i(\vec{x})$ oznaka za $\neg\Theta_i(\vec{x})$, a u suprotnom, ako je formula $\Theta_i(\vec{x})$ negacija atomičke formule $A(\vec{x})$, neka je $\Phi_i(\vec{x})$ oznaka za $A(\vec{x})$ (u oba slučaja je $\Phi_i(\vec{x})$ je ekvivalentno sa $\neg\Theta_i(\vec{x})$, a pri tom su sve formule $\Phi_i(\vec{x})$ $(1 \leq i \leq k)$ literali ; opisana transformacija koristi se kako bi se izbegla dvostruka negacija i korišćenje odgovarajućeg pravila izvođenja):

$$\Theta(\vec{x},\vec{y}) \equiv \neg(\Phi_1(\vec{x}) \wedge \ldots \wedge \Phi_k(\vec{x})) \vee \Phi_{k+1}(\vec{x},\vec{y}) \ldots \vee \Phi_p(\vec{x},\vec{y})$$

Neka je $\Phi(\vec{x})$ kraći zapis za $\Phi_1(\vec{x}) \wedge \ldots \wedge \Phi_k(\vec{x})$, a $\Psi_i(\vec{x},\vec{y})$ za $\Phi_{k+i}(\vec{x},\vec{y})$. Tada je:

$$\Theta(\vec{x},\vec{y}) \equiv \neg\Phi(\vec{x}) \vee (\Psi_1(\vec{x},\vec{y}) \vee \ldots \vee \Psi_q(\vec{x},\vec{y})) \quad (q = p - k)$$

tj:

$$\Theta(\vec{x},\vec{y}) \equiv \Phi(\vec{x}) \Rightarrow (\Psi_1(\vec{x},\vec{y}) \vee \ldots \vee \Psi_q(\vec{x},\vec{y}))$$

Označimo sa $\Psi(\vec{x},\vec{y})$ disjunkciju $\Psi_1(\vec{x},\vec{y}) \vee \ldots \vee \Psi_q(\vec{x},\vec{y})$. Dakle,

$$\forall\vec{x}\exists\vec{y}\Theta(\vec{x},\vec{y}) \equiv \forall\vec{x}\exists\vec{y}(\Phi(\vec{x}) \Rightarrow \Psi(\vec{x},\vec{y}))$$

tj. treba dokazati formulu:

$$\forall\vec{x}\exists\vec{y}(\Phi(\vec{x}) \Rightarrow \Psi(\vec{x},\vec{y})) \tag{2.2}$$

Forma (2.2) odabrana jer se većina geometrijskih teorema uobičajeno formuliše upravo u tom obliku. Za većinu rečenica ova forma nije jedinstveno određena (neka od formula Φ_i $(i \leq k)$ može da bude deo formule Ψ, a ne formule Φ), ali kada postoji više mogućnosti biramo onu koja odgovara tradicionalnom geometrijskom pristupu[1].

Sistem izvođenja iz [Men64, str.57] (uključujući i logičke aksiome) označavaćemo sa M. Ako je iz skupa formula Γ formula $\mathcal{A}$ izvodiva u sistemu izvođenja M zapisavaćemo to na sledeći način:

$$\Gamma \vdash \mathcal{A}.$$

Pretpostavimo da smo dokazali:

$$\Gamma, \Phi'(\vec{a}) \vdash \exists\vec{y}\Psi(\vec{a},\vec{y}) \tag{2.3}$$

(Γ označava skup aksioma teorije $\mathcal{E}'$; $\Phi'(\vec{a})$ označava skup literala $\Phi_1(\vec{a}), \Phi_2(\vec{a}), \ldots, \Phi_k(\vec{a})$; $\vec{a}$ označava nove simbole konstante, ili preciznije, simbole konstanti koji ne pripadaju jeziku u kojem su formulisane aksiome teorije $\mathcal{E}'$ i formule $\Phi(\vec{x})$, $\Psi(\vec{x},\vec{y})$.). Onda važi i:

$$\Gamma, \Phi(\vec{a}) \vdash \exists\vec{y}\Psi(\vec{a},\vec{y}),$$

(gde je $\Phi(\vec{x}) \equiv \Phi_1(\vec{x}) \wedge \ldots \wedge \Phi_k(\vec{x})$) iz čega dalje sledi:

$$\begin{aligned}
&\Gamma \vdash \Phi(\vec{a}) \Rightarrow \exists\vec{y}\Psi(\vec{a},\vec{y}) && \text{([Men64, str.61], teorema o dedukciji)}\\
&\Gamma \vdash \forall\vec{x}(\Phi(\vec{x}) \Rightarrow \exists\vec{y}\Psi(\vec{x},\vec{y})) && \text{([Men64, str.57], generalizacija)}\\
&\Gamma \vdash \forall\vec{x}\exists\vec{y}(\Phi(\vec{x}) \Rightarrow \Psi(\vec{x},\vec{y})) && \text{([Men64, str.85], preneks normal)}
\end{aligned} \tag{2.4}$$

Dakle, da bismo dokazali dokazali teoremu $\forall\vec{x}\exists\vec{y}\Theta(\vec{x},\vec{y})$ dovoljno je dokazati da važi $\Gamma, \Phi(\vec{a}) \vdash \exists\vec{y}\Psi(\vec{a},\vec{y})$[2].

Ako u (2.2) nijedna od formula Φ_i nije literal nad $\vec{x}$, onda, analogno prvom slučaju, dokazujemo $\Gamma \vdash \exists\vec{y}\Psi(\vec{a},\vec{y})$ (pri čemu jeziku teorije treba dodati nove konstante $\vec{a}$) iz čega proizilazi i $\Gamma \vdash \forall\vec{x}\exists\vec{y}\Psi(\vec{x},\vec{y})$ ($\Psi(\vec{x},\vec{y})$ je formula u disjunktvino-normalnoj formi ekvivalentna formuli $\Theta(\vec{x},\vec{y})$).

Slično, teoreme oblika $\forall\vec{x}\Theta(\vec{x})$ zapisujemo u obliku $\forall\vec{x}(\Phi(\vec{x}) \Rightarrow \Psi(\vec{x}))$ (ako je to moguće) ili u obliku $\forall\vec{x}\Psi(\vec{x})$ (Ψ je formula u disjuntivno normalnoj formi) i dokazujemo da važi $\Gamma, \Phi'(\vec{a}) \vdash \Psi(\vec{a})$ odnosno $\Gamma \vdash \Psi(\vec{a})$ (pri čemu jeziku teorije treba dodati nove konstante $\vec{a}$).

Za teoreme oblika $\exists\vec{y}\Theta(\vec{y})$ dokazujemo tvrđenja oblika $\Gamma \vdash \exists\vec{y}\Psi(\vec{y})$ ($\Psi(\vec{y})$ je formula u disjunktvino-normalnoj formi ekvivalentna formuli $\Theta(\vec{y})$).

[1] U samom dokazivaču teoreme se zadaju u formi (2.2) i u njemu se ne vrši opisana transformacija.

[2] U sistemu EUKLID dokazi se izvode u obliku (2.3).

2.2.2 Pravila izvođenja i logičke aksiome

Sistem izvođenja u dokazivaču EUKLID čine sheme osam pravila i jedna logička aksioma.

Pravilo *modus ponens* (MP)[3]:

$$\frac{A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}) \quad \forall \vec{x}(A_1(\vec{x}) \wedge A_2(\vec{x}) \wedge \ldots \wedge A_n(\vec{x}) \Rightarrow \mathcal{D}(\vec{x}))}{\mathcal{D}(\vec{a})}$$

(formule A_i su literali nad nekim od konstanti $\vec{a}$, $\mathcal{D}(\vec{a})$ je formula u disjunktivno-normalnoj formi bez slobodnih promenljivih i bez kvantifikatora).

Pravilo *uvođenje konstanti* (C):

$$\frac{\exists \vec{y} \mathcal{D}(\vec{y}))}{\mathcal{D}(\vec{c})}$$

(gde je $\mathcal{D}(\vec{c})$ formula u disjunktivno-normalnoj formi bez slobodnih promenljivih i bez kvantifikatora; $\vec{c}$ označava nove simbole konstanti: $c_1, c_2, \ldots, c_m$).

Pravilo *modus ponens sa uvođenjem konstanti* (MPC):

$$\frac{A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}) \quad \forall \vec{x} \exists \vec{y}(A_1(\vec{x}) \wedge A_2(\vec{x}) \wedge \ldots \wedge A_n(\vec{x}) \Rightarrow \mathcal{D}(\vec{x}, \vec{y}))}{\mathcal{D}(\vec{a}, \vec{c})}$$

(formule A_i su literali nad nekim od konstanti $\vec{a}$, $\mathcal{D}(\vec{a}, \vec{c})$ je formula u disjunktivno-normalnoj formi bez slobodnih promenljivih i bez kvantifikatora; $\vec{c}$ označava nove simbole konstanti: $c_1, c_2, \ldots, c_m$).

Pravilo *uvođenje činjenica – introductio facta* (IF):

$$\frac{A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), \mathcal{D}_1(\vec{a}) \vee \mathcal{D}_2(\vec{a}) \vee \ldots \vee \mathcal{D}_m(\vec{a}) \quad \begin{matrix}[\mathcal{D}_1'(\vec{a})] \\ \Delta_1\end{matrix} \quad \begin{matrix}[\mathcal{D}_2'(\vec{a})] \\ \Delta_2\end{matrix} \quad \ldots \quad \begin{matrix}[\mathcal{D}_m'(\vec{a})] \\ \Delta_m\end{matrix}}{\Delta}$$

(ako je $\mathcal{D}_i(\vec{a})$ konjunkcija literala $\mathcal{D}_i^1(\vec{a}) \wedge \mathcal{D}_i^2(\vec{a}) \wedge \ldots \wedge \mathcal{D}_i^p(\vec{a})$, onda $[\mathcal{D}_i'(\vec{a})]$ označava uvođenje pretpostavki $\mathcal{D}_i^1(\vec{a}), \mathcal{D}_i^2(\vec{a}), \ldots, \mathcal{D}_i^p(\vec{a})$; simboli Δ_i označavaju ili F (simbol za kontradikciju, "laž") ili neku rečenicu Ψ; u instanci ovog pravila u kojoj svi simboli Δ_i predstavljaju kontradikciju (za $1 \leq i \leq m$), kontradikciju označava i Δ; u instanci ovog pravila u kojoj neki (bar jedan) od simbola Δ_i predstavljaju rečenicu Ψ, a ostali predstavljaju kontradikciju, simbol Δ označava rečenicu Ψ.)

Pravilo *kontradikcija* (F):

$$\frac{A, \neg A}{F} \quad (A \text{ je atomička formula})$$

Pravila *detekcije dokaza* (D1), (D2), (D3):

$$\frac{A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a})}{\Psi_1(\vec{a}) \vee \Psi_2(\vec{a}) \vee \ldots \vee \Psi_q(\vec{a})}$$

[3] Pravilo *modus ponens* u sistemu izvođenja E je specijalna instanca uobičajenog pravila *modus ponens*.

(gde je $\Psi_i(\vec{a}) \equiv A_1(\vec{a}) \wedge A_2(\vec{a}) \wedge \ldots \wedge A_n(\vec{a})$ za neko i)

$$\frac{A_1(\vec{a},\vec{b}), A_2(\vec{a},\vec{b}), \ldots, A_n(\vec{a},\vec{b})}{\exists\vec{y}(\Psi_1(\vec{a},\vec{y}) \vee \Psi_2(\vec{a},\vec{y}) \vee \ldots \vee \Psi_q(\vec{a},\vec{y}))}$$

(gde je $\Psi_i(\vec{a},\vec{b}) \equiv A_1(\vec{a},\vec{b}) \wedge A_2(\vec{a},\vec{b}) \wedge \ldots \wedge A_n(\vec{a},\vec{b})$ za neko i)

$$\frac{A_1(\vec{b}), A_2(\vec{b}), \ldots, A_n(\vec{b})}{\exists\vec{y}(\Psi_1(\vec{y}) \vee \Psi_2(\vec{y}) \vee \ldots \vee \Psi_q(\vec{y}))}$$

(gde je $\Psi_i(\vec{b}) \equiv A_1(\vec{b}) \wedge A_2(\vec{b}) \wedge \ldots \wedge A_n(\vec{b})$ za neko i)

Pored navedenih pravila u sistem izvođenja dokazivača EUKLID ulazi (za klasičnu varijantu) i sledeća logička aksioma – *aksioma isključenja trećeg – tertium non datur* (TND)[4]:

$$A \vee \neg A \quad (A \text{ je atomička formula})$$

U pravilu oblika $\frac{\Gamma}{\Delta}$ skup formula Γ zovemo premisama, a formulu Δ posledicom.

U pravilima (C) i (MPC) $\vec{c}$ označava nove konstante $c_1, c_2, \ldots c_q$ (v. pravilo C [Men64, str.73]). Za tako uvedene konstante kažemo da *zavise* od konstanti $a_1, a_2, \ldots, a_p$.

Pravilo (IF) ima mnoštvo instanci, ali za teoriju $\mathcal{E}'$ broj disjunkata $\mathcal{D}_i$ (i istovremeno broj odgovarajućih grana) – broj m – veći je od 1 samo ako je formula $\mathcal{D}_1(\vec{a}) \vee \mathcal{D}_2(\vec{a}) \vee \ldots \vee \mathcal{D}_m(\vec{a})$ izvedena na osnovu granajućih aksioma $\mathcal{G}_1$ $(m = 3)$, $\mathcal{G}_2$ $(m = 2)$ ili na osnovu aksiome (TND) (m=2). Jedna od takvih je npr. i sledeća instanca pravila (IF):

$$\frac{A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), A \vee \neg A \qquad \overset{[A]}{F} \qquad \overset{[\neg A]}{\Psi(\vec{a})}}{\Psi(\vec{a})}$$

Dokaz izveden sistemom E može se prikazati i u obliku povezanog usmerenog grafa koji ima tačno jedan čvor ka kojem ne vodi nijedna ivica (*početni čvor dokaza*) i tačno jedan čvor iz kojeg ne vodi nijedna ivica (*završni čvor dokaza*). Iz jednog čvora tog grafa vodi više ivica samo ako njemu odgovara primena pravila (IF). U tom čvoru, dokaz se grana na nekoliko poddokaza koji, ponovo na osnovu istog pravila (IF), vode ka jednom čvoru. Svaki usmereni put od početnog do završnog čvora dokaza zovemo *granom dokaza*.

Ako je iz skupa formula Γ primenom navedenih pravila izvodiva formula $\mathcal{A}$ zapisavaćemo to na sledeći način:

$$\Gamma \overset{E}{\vdash} \mathcal{A}.$$

[4] Izostavljanem ove aksiome dobija se intuicionistička varijanta sistema. U geometriji je, međutim, broj teorema koje je moguće dokazati bez korišćenja (u nekoj formi) pravila isključenja trećeg (*tertium non datur*) jako mali.

U izloženom sistemu E, ukoliko je formula $\Phi(\vec{a})$ u kontradikciji sa aksiomama teorije $\mathcal{E}'$, može se dokazati $\Gamma, \Phi'(\vec{a}) \overset{E}{\vdash} F$. Ipak, u nekim takvim situacijama može se (za neku formulu $\Psi(\vec{a}, \vec{y})$) dokazati i $\Gamma, \Phi'(\vec{a}) \overset{E}{\vdash} \exists \vec{y} \Psi(\vec{a}, \vec{y})$. Iako ne u skladu sa konceptom "dobro formiranih odnosa" i relevantne logike, to je u sistemu E (i u većini drugih) ispravno, ali se u tradicionalnim geometrijskim dokazima obično izbegava takvo izvođenje.

Primer 1: Dokažimo sledeću teoremu teorije $\mathcal{E}'$:

$$\forall x \forall y \exists z (p(x) \wedge t(y) \wedge \neg i(x, y) \Rightarrow r(z) \wedge i(x, z) \wedge i(y, z))$$

(Za bilo koju pravu i tačku koja joj nije incidentna postoji ravan kojoj su incidentne.)
Dokaz[5]:

1	$p(a), t(p), \neg i(p,a)$	hipoteze								
2	$t(q_1), t(q_2), \neg q_1 = q_2, i(q_1,a), i(q_2,a)$	1, $\mathcal{P}_6$, (MPC)								
3	$p = q_1 \vee \neg p = q_1$	1, 2, TND, (MP)								
4_1	$p = q_1$ 3, (IF)		4_2	$\neg p = q_1$	3, (IF)					
5_1	$i(p,a)$ 2, 4_1, $\mathcal{I}_3$, (MP)		5_2	$p = q_2 \vee \neg p = q_2$	1,2,TND					
6_1	F 1 , 5_1 , (F) $(A = i(p,a))$		6_{21}	$p = q_2$ 5_2, (IF)		6_{22}	$\neg p = q_2$	5_2, (IF)		
			7_{21}	$i(p,a)$ $2, 6_{21}, \mathcal{I}_3$, (MP)		7_{22}	$r(b), i(p,b), i(q_1,b), i(q_2,b)$	$1, 2, \mathcal{P}_5$,(MPC)		
			8_{21}	F $1, 7_{21}$, (F), $(A = i(p,a))$		8_{22}	$i(a,b)$	$2, 7_{22}, \mathcal{N}_{12}$,(MP)		
						9_{22}	$\exists y(r(y) \wedge i(a,y) \wedge i(p,y))$	$7_{22}, 8_{22}$ (D2)		
11	$\exists y(r(y) \wedge i(a,y) \wedge i(p,y))$ (IF)		10_2	$\exists y(r(y) \wedge i(a,y) \wedge i(p,y))$ (IF)						

Navedimo i odgovarajući dokaz (*more geometrico*) na prirodnom jeziku (videti i sliku 2.1 – prikaz dokaza u obliku grafa):

Na osnovu aksiome $\mathcal{P}_8$ postoje dve tačke incidentne pravoj a (neka su to tačke q_1 i q_2). Tačke p i q_1 su identične ili nisu identične.

Pretpostavimo da su tačke p i q_1 identične. Tačka q_1 je incidentnta pravoj a, a tačke p i q_1 su identične, pa, na osnovu aksioma jednakosti, sledi da je tačka p incidentna pravoj a. Dakle, tačka p je incidentna pravoj a i tačka p nije incidentna pravoj a. Kontradikcija!

Pretpostavimo da tačke p i q_1 nisu identične. Tačke p i q_2 su identične ili nisu identične.

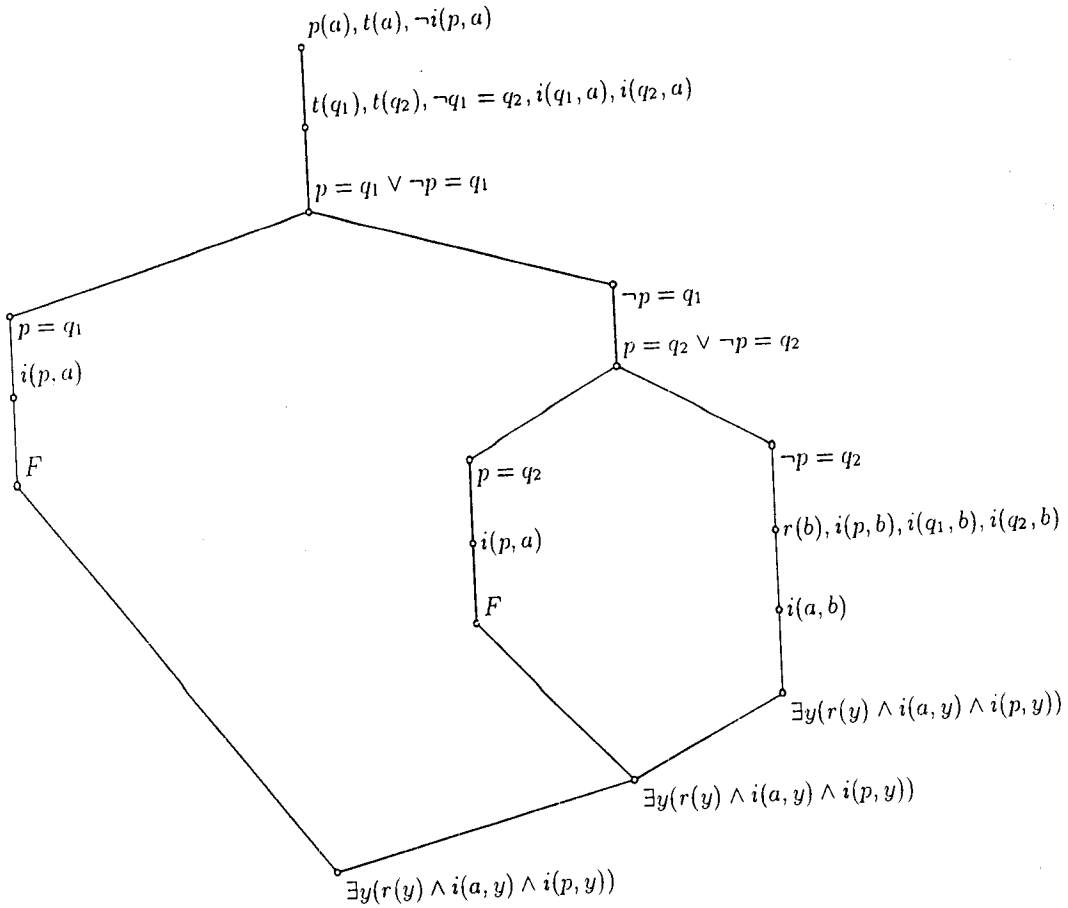
Pretpostavimo da su tačke p i q_2 identične. Tačka q_2 je incidentnta pravoj a, a tačke p i q_2 su identične, pa na osnovu aksioma jednakosti sledi da je tačka p incidentna pravoj a. Dakle, tačka p je incidentna pravoj a i tačka p nije incidentna pravoj a. Kontradikcija!

Pretpostavimo da tačke p i q_2 nisu identične. Na osnovu aksiome $\mathcal{P}_8$ postoji ravan b kojoj su incidentne tačke p, q_1 i q_2. Tačke q_1 i q_2 su incidentne ravni b, pa je, na osnovu aksiome $\mathcal{N}_6$ ravni b incidentna i prava a. Dakle, postoji ravan kojoj su incidentne tačka p i prava a.

Postoji ravan kojoj su incidentne tačka p i prava a.

Postoji ravan kojoj su incidentne tačka p i prava a.

[5]Navedenu teoremu moguće je dokazati i jednostavnije – u manjem broju koraka, ali ovde je izložen dokaz koji ilustruje uvedeni sistem izvođenja E



Slika 2.1

2.2.3 Svojstva sistema izvođenja E

Nedostaci sistema izvođenja E su to što on ne pokriva kompletan predikatski račun i što se pretpostavlja da su formule sa kojima sistem operiše već unapred zapisane na specifičan način (to može biti korigovano dodavanjem novih pravila izvođenja). Pored toga, slično Gencenovom sistemu, sistemu nedostaje određenja formalna elegancija koja proističe iz relativno velikog broja pravila izvođenja (npr. u odnosu na sistem M). S druge strane, sistem E omogućava izvođenje dokaza veoma bliskih uobičajenom zaključivanju u većini matematičkih disciplina (pogotovu u geometriji). Takođe, dokazi koji se izvode u okviru sistema E su ne samo prirodni i intuitivno jasni, već često i bitno kraći od dokaza u drugim sistemima. U ovom poglavlju navešćemo nekoliko svojstava sistema izvođenja E.

Teorema 2.1 (Teorema o dobroj zasnovanosti – *soundness*)

$$\Gamma \overset{E}{\vdash} \mathcal{A} \longrightarrow \Gamma \vdash \mathcal{A}\,.$$

Dokaz: Pravila (MP), (C), (MPC), (F), (D1), (D2), (D3) i aksioma (TND) su kombinacije instanci pravila i teorema sistema izvođenja M, pa ako je neka formula izvodiva primenom ovih pravila u sistemu E, onda je ona očigledno izvodiva i u sistema izvođenja M. Dokažimo npr. da ako je formula izvodiva pravilom (D2) iz nekog skupa formula, onda je ona iz tog skupa formula izvodiva i u sistemu M. Neka je $\Psi_i(\vec{a},\vec{b}) \equiv A_1(\vec{a},\vec{b}) \wedge A_2(\vec{a},\vec{b}) \wedge \ldots \wedge A_n(\vec{a},\vec{b})$ za neko i. U sistemu M važi:

$$\Gamma, A_1(\vec{a},\vec{b}), A_2(\vec{a},\vec{b}), \ldots, A_n(\vec{a},\vec{b}) \vdash \Psi_i(\vec{a},\vec{b})$$

$$\Gamma, \Psi_i(\vec{a},\vec{b}) \vdash \Psi_1(\vec{a},\vec{b}) \vee \Psi_2(\vec{a},\vec{b}) \vee \ldots \vee \Psi_q(\vec{a},\vec{b})$$

$$\Gamma, \Psi_1(\vec{a},\vec{b}) \vee \Psi_2(\vec{a},\vec{b}) \vee \ldots \vee \Psi_q(\vec{a},\vec{b}) \vdash \exists\vec{y}(\Psi_1(\vec{a},\vec{y}) \vee \Psi_2(\vec{a},\vec{y}) \vee \ldots \vee \Psi_q(\vec{a},\vec{y})),$$

odakle sledi i:

$$\Gamma, A_1(\vec{a},\vec{b}), A_2(\vec{a},\vec{b}), \ldots, A_n(\vec{a},\vec{b}) \vdash \exists\vec{y}(\Psi_1(\vec{a},\vec{y}) \vee \Psi_2(\vec{a},\vec{y}) \vee \ldots \vee \Psi_q(\vec{a},\vec{y})),$$

što je i trebalo dokazati.

Matematičkom indukcijom dokazaćemo tvrđenje teoreme za primene pravila (IF), tj. dokazaćemo da ako je iz skupa formula $\Gamma, A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), \mathcal{D}_1(\vec{a}) \vee \mathcal{D}_2(\vec{a}) \vee \ldots \vee \mathcal{D}_m(\vec{a})$ primenom pravila (IF) u sistemu E moguće izvesti formulu ψ, onda je tu formulu moguće izvesti i u sistemu M. Pravilo (IF) može se formulisati i na sledeći način:

Ako važi

$$\Gamma, A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), \mathcal{D}_i'(\vec{a}) \overset{E}{\vdash} \Delta_i \quad (i = 1, 2, \ldots, m) \tag{2.5}$$

onda važi i

$$\Gamma, A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), \mathcal{D}_1(\vec{a}) \vee \mathcal{D}_2(\vec{a}) \vee \ldots \vee \mathcal{D}_m(\vec{a}) \overset{E}{\vdash} \Delta$$

(ako svi simboli Δ_i označavaju kontradikciju, onda kontradikciju označava i simbol Δ; ako bar jedan od simbola Δ_i označava neku formulu ψ, a ostali označavaju kontradikciju, onda simbol Δ označava formulu ψ.)

Za pravilo (IF) primenjeno u nekom dokazu kažemo da je *nivoa* 1, ako su tvrđenja (10) ($i = 1, 2, \ldots, m$) dokazana bez korišenja pravila (IF). Za pravilo (IF) primenjeno u nekom dokazu kažemo da je *nivoa* l, ako se u dokazima tvrđenja (10) koristi pravilo (IF) nivoa l_i ($i = 1, 2, \ldots, m$), ne koristi se pravilo (IF) većeg nivoa i pri tom važi $l = 1 + \max_{i\in\{1,2,\ldots,m\}} l_i$.

Ako se u dokazima tvrđenja (10) ne koristi pravilo (IF) i kako su, kako što je već rečeno, sva pravila sistema E kombinacije instanci pravila i teorema sistema izvođenja M, očigledno je da važi i:

$$\Gamma, A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), \mathcal{D}_i'(\vec{a}) \vdash \Delta_i \quad (i = 1, 2, \ldots, m),$$

odakle proizilazi (na osnovu svojstava sistema M) i

$$\Gamma, A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), \mathcal{D}_1(\vec{a}) \vee \mathcal{D}_2(\vec{a}) \vee \ldots \vee \mathcal{D}_m(\vec{a}) \vdash \Delta$$

(fde simbol Δ označava kontradikciju ako svi simboli Δ_i označavaju kontradikciju, a formulu ψ, ako bar jedan od simbola Δ_i označava formulu ψ, a ostali označavaju kontradikciju: u sistemu M simbol za kontradikciju može biti definisan kao $A \wedge \neg A$, gde je A bilo koja formula.)

Dakle, tvrđenje teoreme važi za dokaze u kojima se javlja pravilo (IF) nivoa 1. Pretpostavimo da tvrđenje teoreme važi i za dokaze u kojima se javljaju primene pravila (IF) nivoa manjih od l ($l \geq 2$) i dokažimo da ono važi i za dokaze u kojima se javlja pravilo (IF) nivoa l.

Pretpostavimo da se primena pravila (IF) i izvođenje

$$\Gamma, A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), \mathcal{D}_1(\vec{a}) \vee \mathcal{D}_2(\vec{a}) \vee \ldots \vee \mathcal{D}_m(\vec{a}) \overset{E}{\vdash} \Delta$$

u nekom dokazu zasniva na tvrđenjima u kojima se javljaju primene pravila (IF) stepena $l_i \quad (i = 1, 2, \ldots, m)$ i pri tome je $l = 1 + \max_{i \in \{1,2,\ldots,m\}} l_i$ (odakle sledi i $l_i < l \quad (i = 1, 2, \ldots, m)$):

$$\Gamma, A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), \mathcal{D}_i'(\vec{a}) \overset{E}{\vdash} \Delta_i \quad (i = 1, 2, \ldots, m).$$

Na osnovu induktivne hipoteze, onda važi i

$$\Gamma, A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), \mathcal{D}_i'(\vec{a}) \vdash \Delta_i \quad (i = 1, 2, \ldots, m),$$

odakle proizilazi (na osnovu svojstava sistema M) i

$$\Gamma, A_1(\vec{a}), A_2(\vec{a}), \ldots, A_n(\vec{a}), \mathcal{D}_1(\vec{a}) \vee \mathcal{D}_2(\vec{a}) \vee \ldots \vee \mathcal{D}_m(\vec{a}) \vdash \Delta,$$

što je i trebalo dokazati.

S obzirom na obrazloženje iz prethodnog poglavlja, iz teoreme **2.1** sledi sledeće tvrđenje: da bismo npr. dokazali da važi

$$\Gamma \vdash \forall \vec{x} \exists \vec{y} \Theta(\vec{x}, \vec{y}) ,$$

tj. da bismo dokazali teoremu

$$\forall \vec{x} \exists \vec{y} \Theta(\vec{x}, \vec{y}) ,$$

odnosno teoremu

$$\forall \vec{x} \exists \vec{y} (\Phi(\vec{x}) \Rightarrow \Psi(\vec{x}, \vec{y})) ,$$

dovoljno je dokazati da važi

$$\Gamma, \Phi'(\vec{a}) \overset{E}{\vdash} \exists \vec{y} \Psi(\vec{a}, \vec{y}) .$$

U ovom tekstu iznesimo i sledeću hipotezu: ako je Γ skup aksioma teorije $\mathcal{E}'$ i ako je $\mathcal{A}$ formula teorije $\mathcal{E}'$ koja ima jednu od sledeće dve forme:

$$\exists \vec{y} \Theta(\vec{a}, \vec{y}),$$

$$\exists \vec{y}\Theta(\vec{y}),$$

(Θ označava formulu teorije $\mathcal{E}'$ bez kvantifikatora i bez slobodnih promenljivih), onda važi:

$$\Gamma \vdash \mathcal{A} \longrightarrow \Gamma \overset{E}{\vdash} \mathcal{A},$$

tj. za navedene klase teorema teorije $\mathcal{E}'$, sistem E ima svojstvo potpunosti.

Primetimo da ako je u nekom čvoru neke grane dokaza primenom pravila (MP) izvedenena formula Ψ, onda taj korak dokaza može biti eliminisan ako je formula Ψ i pre njega bila izvodiva primenom pravila (D1). Slično, ukoliko je u nekom čvoru neke grane dokaza, primenom pravila (C) ili (MPC) izvedena formula $\Psi(\vec{c_2})$ (gde $\vec{c_2}$ označava nove konstante), onda taj korak dokaza može biti eliminisan, ako je i pre njega, primenom pravila (D2) ili (D3) bila izvodiva formula $\Psi(\vec{c_1})$. Od tog čvora dokaza sva pojavljivanja konstanti $\vec{c_2}$ mogu da se zamene konstantama $\vec{c_1}$ i pri tome sva izvođenja ostaju ispravna. Iz navedenih činjenica o tome kako suvišni koraci dokaza mogu biti eliminisani proizilazi i tvrđenje sledeće teoreme važne i za formulaciju algoritma za automatsko izvođenje dokaza:

Teorema 2.2 (Teorema o redukciji)

Ukoliko važi $\Gamma \overset{E}{\vdash} \mathcal{A}$, onda je iz skupa formula Γ, u okviru sistema E, moguće izvesti formulu $\mathcal{A}$ tako da nema koraka dokaza u kojem je primenom pravila (MP) izvedena formula Ψ, a da je pri tom ona mogla da bude izvedena i primenom pravila (D1), kao ni koraka dokaza u kojem su primenom pravila (C) ili (MPC) uvedene nove konstante $\vec{c_2}$, za koje važi $\Psi(\vec{c_2})$, a da je pri tom primenom pravila (D2) ili (D3) mogla da bude izvedena formula $\Psi(\vec{c_1})$ za neke konstante $\vec{c_1}$.

3

ALGORITAM

3.1 Algoritmi za automatsko izvođenje dokaza

Jedan od prvih jasno formulisanih algoritama za automatsko izvođenje dokaza bio je algoritam "British Museum" koji se zasnivao na sukcesivnom sintaksičkom izvođenju svih formula iz onih već dokazanih. U svakom koraku proverava se da li je, među tako generisanim formulama, i ona koja se dokazuje. Već je sistem *Logic Theory Machine* koji su u drugoj polovini pedesetih godina razvili Njuel, Šau i Sajmon (i koji se odnosio na iskazni račun) uključivao i heuristike koje su usmeravale "British Museum" algoritam u skladu sa strukturom teoreme koja se dokazuje (v. [NSS83]). Takođe krajem pedesetih godina, pojavio se i Dželernterov sistem *Geometry Machine* (v. [Gel63], [Gel83]) za dokazivanje jedne (male) klase geometrijskih teorema zasnovan delimično na idejama Marvina Minskog. Pomenuti sistem uveo je dve kvalitativne novine u automatsko dokazivanje teorema. Prva od njih – zaključivanje po analogiji – obezbeđivala je da ako se, u okviru dokaza teoreme, dokaže jedno pomoćno tvrđenje, nakon toga prepoznaju i ne dokazuju analogna tvrđenja. Druga, još značajnija, tehnika uvedena sistemom *Geometry Machine* bilo je tzv. "korišćenje dijagrama". "Dijagram" je, za svaku teoremu koju treba dokazati, predstavljao jednu njenu konkretnu interpretaciju (u skupu realnih brojeva). Hipoteze koje bi, ukoliko se potvrde, mogle da vode ka rešenju problema, proveravaju se najpre na dijagramu i ukoliko su tačne na dijagramu, dokazivač pokušava i formalno da ih dokaže (korišćenjem određenog broja geometrijskih aksioma i teorema). Ovaj sistem je i pored brojnih nedostataka (između ostalog, mogao je da dokazuje samo veoma jednostavne teoreme koje se odnose na podudarnost trouglova) ostavio traga u automatskom dokazivanju teorema i ideje koje su ovim sistemom uvedene, primenjivane su, pored geometrije, i u drugim domenima. Jedan od prvih sistema za automatsko dokazivanje teorema bio je i značajni sistem koji je 1960. godine razvio Pol Gilmor i koji je bio zasnovan na Herbrandovoj teoremi i njenim implikacijama[1] (v.npr. [Bu87,str.278). Pomenuti sistemi bili su prilično neefikasni i mogli su da dokažu samo veoma jednostavne

[1] Herbrandova teorema, između ostalog, sugeriše tzv. "dokaz negiranjem" tj. dodavanje negacije zadatog tvrđenja kao nove aksiome i traganje za kontradikcijom, umesto traganja za tvrđenjem između onih koji se generišu. Taj pristup prihvaćen je i u metodama tabloa i rezolucije.

teoreme, ali su, ipak, pokazali da je automatsko dokazivanje teorema moguće ("bar u principu") i to je bio dovoljan podstrek za dalja istraživanja. Nekoliko godina kasnije pojavio se jedan od ključnih rezultata – metod koji je donekle bio zasnovan na metodologiji Herbranda i Gilmoura, ali znatno efikasniji – bio je to metod rezolucije Alena Robinsona (v. [Ro60]). Metod rezolucije razrešio je neke od problema koji su uslovljavali neefikasnost Gilmourovog sistema. Uobičajene aksiome i pravila izvođenja predikatskog računa zamenjena su samo jednim, relativno komplikovanim, pravilom nazvanim *pravilo rezolucije* koje je uključivalo i novu značajnu proceduru – *unifikaciju*. Broj teorema različitih matematičkih teorija koje je bilo moguće automatski dokazati bitno je povećan, a kada je u cilju daljeg povećanja efikasnosti uvedeno i dodatno pravilo izvođenja - *paramodulacija*, činilo se da će proces kontinuiranog napretka automatskog dokazivanja teorema na osnovama postavljenim metodom rezolucije teći i dalje, nalazeći primene u različitim oblastima: ispitivanju postavljenih matematičkih hipoteza, u verifikaziji programa, obradi prirodnog jezika, obrazovanju, svakodnevnog rezonovanja itd. Tokom druge polovine šezdesetih i početkom sedamdesetih godina implementirani su mnogi sistemi ("zvučnih imena") za automatsko dokazivanje teorema zasnovani na metodi rezolucije koji su uključivali specifičan izbor aksioma i klauza za rezoluciju, kao i brojne heuristike, ali kako je i sa tim unapređenjima i dalje bilo moguće dokazati samo veoma jednostavne teoreme, prvobitno oduševljenje i očekivanja od automatskog dokazivanja teorema počeli su da opadaju. Pored toga što su ovi sistemi uglavnom veoma neefikasni, dokazi koje su generisali ovi metodi, iako matematički korektni, bili su po svojoj strukturi daleko od uobičajenih dokaza, i praktično jedini upotrebljiv rezultat bio je potvrdan ili odrečan odgovor na pitanje da li je zadato tvrđenje teorema. Ipak, metoda rezolucije ostavila je veliki trag na razvoj automatskog dokazivanja teorema i veštačke inteligencije. Ideje i tehnike uvedene metodom rezolucije tokom šezdesetih i sedamdesetih godina i danas se koriste u logici i računarstvu. Jedan od najznačajnijih tragova tog perioda, svakako je i koncept deskriptivnog programiranja i jezik PROLOG koij je neposredni rezultat razvoja metode rezolucije.

Kako su, pogotovu pod snažnim uticajem istraživača sa univeziteta MIT, jačale sumnje u visoke domete "ravnomernih procedure dokaza" (*uniform proof procedures*) koje su dominirale šezdesetih i sedamdesetih godina (pored metoda rezolucije i metod tabloa), istraživanja su sve više išla ka izgradnji specifičnih sistema koji su prilagođeni konkretnim teorijama i često, samo delovima tih teorija (v.npr. algoritme za Prezburger i Bledso realnu aritmetiku u [Bu83,str.132], [Bl77], [Sh77] ili [Sh79]). U grupi tih dokazivača i algoritama, razvijanih osamdesetih i devedesetih godina, svojom efikasnošću ističe se Vuov algoritam za dokazivanje geometrijskih teorema algebarskim metodama (v. [Ch88]). Nedostacima ovog elegantnog algoritma (suštinski, svodi se na deljenje polinoma) možemo da smatramo to što nema svojstvo potpunosti (neke teoreme ne može da dokaže) i to što se u dokazima koje generiše ne može prepoznati uobičajeni geometrijski smisao (u dokazu se i ne koriste uobičajene geometrijske aksiome). Ipak, kako ovaj algoritam može veoma efikasno (na današnjim PC računarima za svega nekoliko sekundi) da dokaže brojne netrivijalne i često izuzetno komplikovane teoreme, on verovatno predstavlja najveći domet u automatskom dokazivanju teorema geometrije, a možda i u automatskom dokazivanju teorema uopšte.

Možemo da smatramo da su tri ključna kriterijuma za ocenu kvaliteta algoritma za automatsko dokazivanje teorema svojstvo potpunosti, efikasnost i forma izvedenih dokaza

(uobičajena, prirodna forma ili ne). Ovi kriterijumi su, međutim, u velikoj meri, u suprotnosti jedan sa drugim, pa i ne postoji algoritam koji u značajnoj meri zadovoljava sva tri zahteva. Tako, npr. metod rezolicije i metod tabloa imaju svojstvo potpunosti, ali su neefikasni, dok je Vuov algoritam izuzetno efikasan, ali nema nema svojstvo potpunosti. Pri tome, dokazi izvedeni korišćenjem sve tri pomenute metode ne odgovaraju uobičajenom ljudskom rasuđivanju.

3.2 Algoritam izvođenja dokaza u dokazivaču EUKLID

Aksiomatski sistem geometrije izložen u prvom i sistem izvođenja dokaza izložen u drugom delu ovog rada čine osnovu algoritma za izvođenje dokaza u sistemu EUKLID. Taj algoritam nezavistan je od konkretne računarske realizacije, ali i od računarske primene uopšte. Algoritam pokriva jednu klasu teorema teorije $\mathcal{E}'$ (koja sadrži značajni deo standardnih geometrijskih sadržaja), i razvijen je sa ciljem da generisani dokazi u potpunosti odgovaraju tradicionalnim dokazima, uobičajenim u matematici dve i po hiljade godina. Prioritet je dat tom kriterijumu na račun efikasnosti. U osnovnoj verziji dokazivača usmeravanje procesa dokazivanja zasniva se na klasifikaciji aksioma i njihovom poretku u okviru grupa, ali sam koncept ostavlja prostor i za primenu drugih heuristika i tehnika usmeravanja. U ovom tekstu nećemo se baviti tim pitanjima, već ćemo razmatrati samo osnovni oblik algoritma.

U algoritmu se koristi pojam *dopustivi objekti* proistekao iz tzv. *principa graničnika* upotrebljenog u dokazivaču. Na početku izvođenja dokaza, skup dopustivih objekata je prazan i tokom izvođenja dokaza taj skup se proširuje pod kontrolom graničnika koji onemogućava pojavljivanje "beskonačnih grana" u dokazu.

Tokom izvođenja dokaza proširuje se, sukcesivnom primenom aksioma tzv. *prostor znanja* koji sadrži činjenice o objektima čija je egzistencija utvrđena (tj. izvedene formule nad konstantama). Pri grananju dokaza, prostor znanja proširuje se i pretpostavkama tekuće grane. Ovakav koncept odgovara sintaktičkom pristupu reprezentaciji znanja u veštačkoj inteligenciji i razlikuje se od koncepta *closed-world assumption* (v.npr. [AI87]), jer npr. ako u prostoru znanja ne postoji informacija o tome da se dve prave seku, to još uvek ne znači da se one zaista ne seku; na taj način ostvaruje se princip *monotonog rasuđivanja* (*monotonic reasoning*; v.npr. [AI87]). U toku izvođenja dokaza, geometrijske i dodatne aksiome, definicije i teoreme (navedene u poglavlju 1.4.1) primenjuju se po pravilima izvođenja navedenim u poglavlju 2.2.2.

Navedeni algoritam omogućava izvođenje dokaza za sve teoreme elementarne geometrije koje mogu biti interpretirane u posebnoj formi (v. poglavlje 2.2), pri čemu se koriste samo osnovni predikati i predikati definisani u poglavlju 1.4.1[2]

Algoritam za izvođenje dokaza je (donekle) zasnovan na "metodi iscrpljivanja". Da bi se maksimalno ograničilo uvođenje novih geometrijskih objekata i činjenica nepotrebnih za dokaz i da bi se povećala efikasnost, aksiome su podeljene u grupe i poređane u okviru svake od njih (kao što je to objašnjeno u prvom delu). Takva podela aksioma dala je u izvođenju dokaza dobre rezultate (po pitanju efikasnosti i malog broja suvišnih koraka) i odredila novu

[2] Od teorema elementarne geometrije iz [Lu94] koje ne zahtevaju upotrebu prirodnih ili realnih brojeva, u navedenom obliku moguće je zapisati većinu njih.

klasifikaciju geometrijskih aksioma. (Dobijeni dokazi, naravno, mogu biti i (automatski) optimizovani, tako da ne sadrže nepotrebne korake, ali u ovom tekstu nećemo se baviti tim problemom.)

Dokazivač EUKLID tokom izvođenja nekog dokaza sve novouvedene objekte označava redom prirodnim brojevima. Time se, efektivno generiše prebrojiv model teorije $\mathcal{E}'$ i to onaj njegov deo koji je potreban za konkretni dokaz. Nezavisno od bilo koje pojedinačne teoreme, algoritam EUKLID može, dakle, u beskonačnom (ali rekurzivnom) postupku da generiše prebrojiv model elementarne geometrije. Postojanje prebrojivog modela teorije $\mathcal{E}'$ proizilazi iz poznate teoreme (v.[Men64,str.65]), ali se algoritmom EUKLID takav model i efektivno konstruiše. Odatle proističe i zanimljiv problem pronalaženja prebrojivog modela teorije $\mathcal{E}'$ koji se može jednostavno i efektivno opisati konačnim postupkom.

Navedeni algoritam (i njegova računarska implementacija) dosledno obezbeđuje strogi formalistički pristup - dokazi se izvode bez veze sa semantikom koju obično pripisujemo geometrijskim dokazima. Iz toga proizilazi i određeni "nesklad" između sintakse i semantike koji se javlja u nekim dokazima izvedenim na osnovu izloženog algoritma (v. poglavlje 2.2.2).

3.2.1 Prostor znanja

U svakom koraku izvođenja dokaza u sistemu EUKLID (primenom aksiome isključenja trećeg i pravila (MP), (C), (MPC) navedenih u poglavlju 2.2.2) kao posledica se, na osnovu zadovoljenih pretpostavki određenog pravila, izvodi neka formula u disjunktivno-normalnoj formi bez kvantifikatora $\mathcal{D}(\vec{a}) \equiv \mathcal{D}_1(\vec{a}) \vee \mathcal{D}_2(\vec{a}) \vee \ldots \vee \mathcal{D}_n(\vec{a})$ ($\mathcal{D}_i(\vec{a})$ su konjunkcije literala). Neka je $\mathcal{D}_k(\vec{a}) \equiv \mathcal{D}_k^1(\vec{a}) \wedge \mathcal{D}_k^2(\vec{a}) \wedge \ldots \wedge \mathcal{D}_k^m(\vec{a})$ (formule $\mathcal{D}_k^j(\vec{a}$ su literali). Kada je dokazana formula $\mathcal{D}(\vec{a})$, primenom pravila izvođenja (IF) dokaz se grana na n poddokaza, pri čemu se u i-toj grani kao pretpostavka uvodi formula $\mathcal{D}_i(\vec{a})$ koja je konjunkcija literala $\mathcal{D}_k^1(\vec{a})$, $\mathcal{D}_k^2(\vec{a})$ $\ldots \mathcal{D}_n^m(\vec{a})$. U toj grani dokaza smatra se da su navedeni literali dokazane *činjenice* i one se uvode (pojedinačno, a ne njihova konjunkcija) u skup dokazanih činjenica - u tzv. *prostor znanja*. Ovako uvedene činjenice brišu se iz prostora znanja kada se završi taj poddokaz. (U jednom takvom koraku, poredak uvedenih činjenica u prostor znanja nije bitan i ako u njemu postoje dva literala A i B, smatra se da su tačne i formula $A \wedge B$ i formula $B \wedge A$.) Ako se dokazuje tvrđenje oblika

$$\Gamma, \Phi(\vec{a}) \overset{E}{\vdash} \exists \vec{y} \Psi(\vec{a}, \vec{y})$$

ili oblika

$$\Gamma, \Phi(\vec{a}) \overset{E}{\vdash} \Psi(\vec{a}),$$

gde je $\Phi(\vec{a}) \equiv \Phi_1(\vec{a}) \wedge \Phi_2(\vec{a}) \wedge \ldots \wedge \Phi_n(\vec{a})$ ($\Phi_i(\vec{a})$ su literali), na samom početku izvođenja dokaza dodaju se oznake za nove konstante $\vec{a}$, a u prostor znanja se upisuju činjenice $\Phi_1(\vec{a})$, $\Phi_2(\vec{a})$, $\Phi_n(\vec{a})$.

Na opisani način, u dokazivaču EUKLID obezbeđena je monotonost zaključivanja (u svakoj grani dokaza). To znači da se u jednoj grani dokaza pri dodavanju nove činjenice u prostor znanja iz njega ne izbacuje neka druga (tj. skup dokazanih činjenica u svakog grani dokaza monotono raste).

3.2.2 Dopustivi objekti i princip graničnika

Primena pravila izvođenja (izuzev pravila (C)) pretpostavlja postojanje određenih konstanti i činjenica koje se na njih odnose (odnosno formula bez kvantifikatora). Reći ćemo da uvedene konstante označavaju *objekte* i označavaćemo ih rednim brojevima redom kako ih uvodimo. Neka od pravila izvođenja primenjivaćemo samo na jednom, posebno definisanom, podskupu objekata – podskupu koji ćemo zvati *dopustivi objekti*. Svi objekti označeni su rednim brojevima i u jednom trenutku tokom izvođenja dokaza dopustivi su oni koji su označeni brojem manjim od vrednosti tzv. *graničnika*. Tokom izvođenja dokaza vrednost graničnika može da se menja i to na način opisan u samom algoritmu.

3.2.3 Aksiome i ADT modul

U dokazivaču EUKLID, pored geometrijskih aksioma koriste se i aksiome zasnovanosti (implicitno), aksiome jednakosti, kao i nekoliko definicija i jednostavnih teorema (v.poglavlje 1.4.1). Sve one čine tzv. ADT modul i po uvedenoj klasifikaciji imaju svojstvo "neproduktivnosti" (sa izuzetkom nekoliko teorema koje se odnose na egzistenciju četiri tačke, na egistenciju tri tačke incidentne nekoj ravni, odnosno dve tačke incidentne nekoj pravoj – njih ćemo, jednostavnosti radi, smatrati dodatnim geometrijskim produktivnim aksiomama, a ne elementima ADT modula).

Aksiome zasnovanosti u dokazivaču se ne koriste eksplicitno. Naime, u svakoj aksiomi u kojoj se uvodi novi geometrijski objekt, uvodi se i njegov (jedinstveni) "tip". Pored toga, nije moguće da se primenom neke aksiome izvede neka formula, a da pre toga nisu utvrđeni tipovi njenih argumenata. Ako, dakle, u skupu aksioma proširenom premisama nema konstanti a za koje nema tačno jedne od formula $\mathcal{S}(a)$, $\mathcal{L}(a)$ ili $\mathcal{P}(a)$, onda nema potrebe za eksplicitnim korišćenjem aksioma zasnovanosti. Sa tim ograničenjem svaka formula $\exists\vec{y}\Theta(\vec{a},\vec{y})$ može biti zapisana u obliku $\exists\vec{y}(\Phi(\vec{a}) \Rightarrow \Psi(\vec{a},\vec{y}))$, a formula $\Theta(\vec{a})$ može biti zapisana u obliku $\Phi(\vec{a}) \Rightarrow \Psi(\vec{a})$ (formula Φ sadrži (bar) predikate o "tipovima" konstanti $\vec{a}$; v.poglavlje 2.2.2). Dokazivač pretpostavlja ovo ograničenje, pa su tvrđenja koja se dokazuju jednog od sledećih oblika:

$$\Gamma, \Phi'(\vec{a}) \overset{E}{\vdash} \exists\vec{y}\Psi(\vec{a},\vec{y}) ,$$

$$\Gamma, \Phi'(\vec{a}) \overset{E}{\vdash} \Psi(\vec{a})$$

$$\Gamma \overset{E}{\vdash} \exists\vec{y}\Psi(\vec{y}) .$$

3.2.4 Pravila izvođenja i klasifikacija aksioma

Pravila izvođenja navedena u poglavlju 2.2.2 prilagođena su uobičajenim (tradicionalnim) geometrijskim dokazima i prirodno odgovaraju srukturi geometrijskih aksioma. Tako se za "primenu" produktivnih i granajućih aksioma koristi pravilo (MPC), neproduktivnih pravilo (MP), a jako produktivnih pravilo (C). Formule izvedene primenom ovih pravila uvode se

u prostor znanja primenom pravila (IF), dok se pravila (F), (D1), (D2), (D3) koriste za "proveru" da li je zadata teorema dokazana. Aksioma isključenja trećeg (TND) primenjuje se po pravilu (MP).

3.2.5 Izvođenje dokaza i teorema o redukciji

Na osnovu teoreme **2.2** (teorema o redukciji) sledi da, ako u okviru sistema E postoji dokaz neke teoreme, onda je tu teoremu moguće dokazati tako da nema koraka dokaza u kojem je primenom pravila (MP) izvedena formula Ψ, a da je pri tom ona mogla da bude izvedena i primenom pravila (D1), kao ni koraka dokaza u kojem su primenom pravila (C) ili (MPC) uvedene nove konstante $\vec{c_2}$, za koje važi $\Psi(\vec{c_2})$, a da je pri tom primenom pravila (D2) ili (D3) mogla da bude izvedena formula $\Psi(\vec{c_1})$ za neke konstante $\vec{c_1}$. Iz teoreme, dakle, sledi da u dokazu nije potrebno primenjivati pravila izvođenja koja su u gore opisanom smislu suvišna. U samom algoritmu smatraćemo da takva pravila izvođenja nisu moguća.

3.2.6 Algoritam za izvođenje dokaza teoreme

Ako se dokazuje tvrđenje

$$\Gamma, \Phi'(\vec{a}) \overset{E}{\vdash} \exists \vec{y} \Psi(\vec{a}, \vec{y})$$

ili

$$\Gamma, \Phi'(\vec{a}) \overset{E}{\vdash} \Psi(\vec{a}),$$

gde je $\Phi(\vec{a}) \equiv \Phi_1(\vec{a}) \wedge \Phi_2(\vec{a}) \wedge \ldots \wedge \Phi_n(\vec{a})$ ($\Phi_i(\vec{a})$ su literali), na samom početku izvođenja dokaza uvode se novi objekti $a_1, a_2, \ldots, a_m$ i označavaju rednim brojevima $1, 2, \ldots, m$, a u prostor znanja se upisuju činjenice $\Phi_1(\vec{a})$, $\Phi_2(\vec{a})$, $\Phi_n(\vec{a})$. Na samom početku izvođenja dokaza nijedan objekt nije dopustiv.

Ako se dokazuje tvrđenje

$$\Gamma \overset{E}{\vdash} \exists \vec{y} \Psi(\vec{y})$$

na samom početku izvođenja dokaza prostor znanja je prazan i nijedan objekt nije dopustiv.

(1) Proveri da li u prostoru znanja postoje dve kontradiktorne činjenice odnosno pokušaj da primeniš pravilo izvođenja (F); ukoliko uspeš, time je završen poddokaz po tekućoj grani, u suprotnom – pređi na korak (2);

(2) Proveri da li je moguće primenom pravila (D_1), (D_2) ili (D_3) izvesti formulu koju treba dokazati; ako jeste time je završen poddokaz po tekućoj grani, u suprotnom – pređi na korak (3);

(3) Pokušaj da, po pravilu (MP), primeniš neki od članova ADT modula; ako uspeš, onda za izvedenu formulu (koja je konjunkcija literala), po pravilu (IF), uvedi kao činjenice odgovarajuće literale i pređi na korak (1); u suprotnom – pređi na korak (4);

(4) Pokušaj da (po pravilu (MP)) primeniš neku od neproduktivnih aksioma; ako uspeš, onda za izvedenu formulu (koja je konjunkcija literala), po pravilu (IF), uvedi kao činjenice odgovarajuće literale i pređi na korak (1); u suprotnom – pređi na korak (5);

(5) Ukoliko u prostoru znanja ne postoji ni činjenica A ni činjenica $\neg A$, primeni aksiomu (TND) i po pravilu (IF) uvedi kao činjenice A, odnosno $\neg A$ i izvedi poddokaz u oba slučaja; u suprotnom pređi na korak (6);[3]

(6) Pokušaj da (po pravilu (MPC)) primeniš neku od granajućih aksioma nad skupom dopustivih objekata; ako uspeš, onda za izvedenu formulu u disjuntivno-normalnoj formi, po pravilu (IF), uvedi kao činjenice odgovarajuće literale i izvedi poddokaz za svaki disjunkt; u suprotnom – pređi na korak (7);

(7) Pokušaj da (po pravilu (MPC)) primeniš neku od produktivnih aksioma nad skupom dopustivih objekata; ako uspeš, onda za izvedenu formulu (koja je konjunkcija literala), po pravilu (IF), uvedi kao činjenice odgovarajuće literale i pređi na korak (1); u suprotnom – pređi na korak (8);

(8) Pokušaj da (po pravilu (C)) primeniš neku od jako produktivnih aksioma; ako uspeš, onda za izvedenu formulu (koja je konjunkcija literala), po pravilu (IF), uvedi kao činjenice odgovarajuće literale i pređi na korak (1); u suprotnom – pređi na korak (9);

(9) Od svih objekata označenih brojevima većim od trenutne vrednosti graničnika odaberi onaj koji je označen najmanjim brojem i dodaj ga skupu dopustivih objekata, tj. dodeli graničniku njegovu vrednost; idi na korak (1).

(Ukoliko se zamene mesta koracima (8) i (9) algoritma dobija se efikasnija verzija dokazivača za jedanu podklasu teorema, ali za ovu verziju ne važi tvrđenje teoreme **3.1**. Pored razlike u strukturi produktivnih i jako produktivnih aksioma, to je drugi razlog za razdvajanje koraka (7) i (8).)

[3] Aksioma (TND) i ovaj korak algoritma ne primenjuju se na predikate $\mathcal{S}$, $\mathcal{L}$, $\mathcal{P}$ (v.poglavlje 3.2.3) niti na predikat $\mathcal{B}$ (jer aksiome kojima se uvodi predikat $\mathcal{B}$ predstavljaju odgovarajuću zamenu).

Primetimo da aksiomu (TND) i ovaj korak nije neophodno primenjivati ni na predikate *kolin*, *kompl* i $\cong$. Zaista, umesto da se uvode pretpostavke $kolin(A,B,C)$ i $kolin(A,B,C)$, mogu se uvesti ekvivalentne pretpostavke $\mathcal{I}(C,p)$ i $\neg\mathcal{I}(C,p)$, gde je p prava kojoj su incidentne tačke A i B (analogno za predikat *kompl*). Umesto da se uvode pretpostavke $(A,B)\cong(C,D)$ i $\neg(A,B)\cong(C,D)$, mogu se uvesti pretpostavke $D=E$ i $\neg D=E$, gde je tačka kolinearna sa tačkama C i D, takva da je $(A,B)\cong(C,E)$ i $\neg\mathcal{B}(D,C,E)$ (takva tačka postoji). Pretpostavke $(A,B)\cong(C,D)$ i $D=E$ su ekvivalentne jer je u sistem uvrštena teorema:

Za svake tri tačke X, Y i Z, ako važi $\mathcal{B}(X,Y,Z)$, onda ne važi $(X,Y)\cong(X,Z)$.

U dokazivaču se ovaj korak primenjuje u skladu sa obrazložim ograničenjima i to bitno smanjuje grananje dokaza i samim tim povećava efikasnost dokazivača.

Ovaj korak algoritma primenjuje se (sem na osnovne predikate $=$ i $\mathcal{I}$) i na izvedeni predikat *seku_se*, jer bi u protivnom morale da se uvode pretpostavke tipa $\exists A(\mathcal{I}(A,a)\wedge\mathcal{I}(A,b))$ i $\neg\exists A(\mathcal{I}(A,a)\wedge\mathcal{I}(A,b))$ koje uključuju kvantifikatore i nisu literali.

3.2.7 Teorema o domenu

Teorema 3.1 Ako važi

$$\Gamma \overset{E}{\vdash} \Phi$$

onda algoritam EUKLID može iz skupa formula Γ da izvede formulu Φ, ili (eventualno) kontradikciju (ukoliko je skup formula Γ protivrečan).

Dokaz:
Pretpostavimo da važi

$$\Gamma \overset{E}{\vdash} \Phi$$

tj. da u sistemu E postoji dokaz formule Φ iz skupa formula Γ. Razmotrimo proizvoljnu granu tog dokaza. Reći ćemo da je dubina početnog čvora te grane 0 i da je $d+1$ dubina neposrednog potomka čvora čija je dubina d.

Neka je v čvor dubine d koji pripada toj grani i neka je w njegov neposredni potomak. Pretpostavimo da algoritam u jednom trenutku izvođenja, u prostoru znanja sadrži sve formule uvedene pretpostavkama ili izvedene pre čvora w u grani dokaza koju razmatramo. S obzirom na stukturu dokaza u sistemu E i na strukturu pravila (IF), dovoljno je dokazati da svi putevi grafa dokaza koji generiše algoritam i koji vode od tekućeg čvora sadrže ili izvedenu formulu Φ ili izvedenu kontradikciju.

Ukoliko čvoru w odgovara primena pravila (F), onda će i u algoritmu biti primenjena ista (ili neka druga) instanca pravila (F) (korak (1) algoritma).

Ukoliko čvoru w odgovara primena pravila (D1), (D2), odnosno (D3) (u skladu sa formom formule Φ), onda će i u algoritmu biti primenjena ista instanca pravila (D1), (D2), odnosno (D3) (korak (2) algoritma).

Ukoliko čvoru w odgovara primena pravila (MP), (MPC) ili (IF) nad nekim konstantama, onda će u konačno mnogo koraka algoritma sve te konstante da postanu dostupne i u konačno mnogo koraka će biti primenjeno pravilo koje odgovara čvoru w ili će u međuvremenu biti dokazana formula Φ (ili, eventualno, kontradikcija).

Ukoliko čvoru w odgovara primena pravila (C), kako je nad konačnim skupom dostupnih konstanti moguće konačno puta primeniti instance pravila (MP), (MPC) ili (IF), pre promene vrednosti graničnika biće primenjene i sve moguće instance pravila (C) (pa i ona koja odgovara čvoru w) ili će u međuvremenu biti dokazana formula Φ (ili, eventualno, kontradikcija).

(Ukoliko se u algoritmu primene pravila (IF), onda će u svakoj grani da bude primenjeno pravilo koje odgovara čvoru w ili će, u tom poddokazu, biti dokazana tražena formula (ili, eventualno, kontradikcija.)

Kako na početku primene algoritma prostor znanja sadrži sve formule Γ, primenom matematičke indukcije zaključujemo da će, ukoliko postoji dokaz formule Φ, algoritam primeniti svaki korak tog dokaza ili će formulu Φ dokazati na drugi način (ili će, ukoliko je skup formula Γ protivrečan, eventualno, izvesti kontradikciju).

4

PROGRAM

4.1 Program EUKLID - verzija na programskom jeziku PROLOG

U PROLOG verziji dokazivača EUKLID, prostor znanja predstavljen je skupom proloških činjenica koje se dodaju odnosno brišu iz njega predikatima `assertz`, odnosno `retract` . Prostor znanja proširuje se, na osnovu pravila (IF), i (eventualno) u nekoliko grana koje predstavljaju poddokaze. Kada je završen jedan poddokaz, iz prostora znanja brišu se sve činjenice koje su pretpostavljene ili izvedene u odgovarajućoj grani. Unarnim geometrijskim predikatima ($\mathcal{S}, \mathcal{L}$ i $\mathcal{P}$) odgovaraju unarni prološki predikati (`t`, `p`, `r`) čiji je argument indeks odgovarajuće uvedene konstante. Preostalim geometrijskim predikatima odgovaraju prološki predikati arnosti veće za po jedan. Taj, dodatni argument predstavlja indeks izvedene činjenice i koristi se za pomenuto brisanje činjenica iz prostora znanja. Vrednost graničnika predstavljena je činjenicom oblika `br(g)` gde je g konstanta koja ima vrednost indeksa nekog od geometrijskih objekata u skladu sa glavnim algoritmom. Aksiome su predstavljene pravilima koja uključuju upis u prostor znanja i ispis odgovarajućeg koraka dokaza na prirodnom jeziku.

```
ax_s(1) :- t(X),p(Y),e(X,Y,_),e(Y,Z,_),not(e(X,Z,_)),dodaj(e(X,Z)),
        stampaj([n_,p_,'Posto je tacka ',X,' incidentna pravoj ',
        Y,' i prava ',Y,
        n_,p_, 'incidentna ravni ',Z,' sledi da je tacka ',X,
        ' incidentna ravni ',Z,'.']).
```

Zapis jedne od aksioma u PROLOG verziji dokazivača EUKLID

```
dokaz :- kontradikcija.
dokaz :- dokazano.
dokaz :- ax_s(M),dokaz.
dokaz :- ax_n(M),dokaz.
dokaz :- pretpostavka(P,NeP),
```

```
        br(B),
        ((IP=true,INeP=true,dokazp([P,NeP]));
        (IP=true,INeP=false,dokazp([P]));
        (IP=false,INeP=true,dokazp([NeP]))).
dokaz :- ax_g(M).
dokaz :- ax_p(M),dokaz.
dokaz :- ax_jp(M),dokaz.
dokaz :- granica(G),
        prvi_objekt(G,N),N1 is N+1,
        retract(granica(G)),
        assert(granica(N1)),
        dokaz.
```

Ključni predikat u PROLOG verziji dokazivača EUKLID

4.2 Program EUKLID - verzija na programskom jeziku C

U C verziji dokazivača EUKLID, prostor znanja predstavljen je skupom nizova koji odgovaraju osnovnim i definisanim predikatima teorije $\mathcal{E}'$ (svakom predikatu odgovaraju dva niza – po jedan za pozitivnu i negativnu formu). Svaki od tih nizova karakteriše i indeks poslednjeg člana koji pripada prostoru znjanja. Činjenice se dodaju u prostor znanja u odgovarajućem nizu na prvoj poziciji posle one označene karakterističnim indeksom, a "brišu" se jednostavnom promenom vrednosti karakterističnog indeksa (svaki od nizova, u skladu sa glavnim algoritmom funkcioniše kao LIFO lista). (Statičkoj organizaciji podataka data je prednost nad dinamičkom zbog brzine koju pružaju jednostavne operacije dodavanja nove činjenice i "brisanje" poslednje dodate.) Prostor znanja proširuje se, na osnovu pravila (IF), i (eventualno) u nekoliko grana koje predstavljaju poddokaze. Kada je završen jedan poddokaz, iz prostora znanja brišu se sve činjenice koje su pretpostavljene ili izvedene u odgovarajućoj grani. Unarnim geometrijskim predikatima ($\mathcal{S}, \mathcal{L}$ i $\mathcal{P}$) odgovaraju nizovi (`POINT[]`, `LINE[]`, `PLANE[]`) struktura `struct object` koje imaju samo jedan član koji ima vrednost indeksa odgovarajuće uvedene konstante. Svakom od preostalih geometrijskih predikata pridružena su dva niza (za pozitivni i negativni oblik) struktura `struct rel_2`, `struct rel_3` ili `struct rel_4` (u zavisnosti od arnosti predikata). Elementi ovih nizova, osim članova koji su jednaki indeksima geometrijskih objekata za koje je izveden (odnosno pretpostavljen) određeni literal, imaju i jedan dodatni član. Taj, dodatni član predstavlja indeks izvedene činjenice i koristi se za pomenuto brisanje činjenica iz prostora znanja. Vrednost graničnika predstavljena je globalnom konstantom `SENT` koja ima vrednost indeksa nekog od geometrijskih objekata u skladu sa glavnim algoritmom. Aksiome su predstavljene funkcijama koje uključuju pozive funkcija za upis u prostor znanja i ispis odgovarajućeg koraka dokaza na prirodnom jeziku.

```
int ax_n10()
{
int i1,i2;
int x,y,z;
for(i1=1;i1<=INC[0].index;i1++)
  {
    x=INC[i1].arg1; y=INC[i1].arg2;
    for(i2=1;i2<=INC[0].index;i2++)
      if (INC[i2].arg1==y)
        {
          z=INC[i2].arg2;
          if (!inc(x,z))
            {
              add_inc(x,z);
              sprintf(OUT,"Posto je tacka %i incidentna pravoj %i i ",x,y);
              sprintf(OUT,"prava %i je incidentna ravni %i, ",z,y);
              sprintf(OUT,"sledi da je tacka %i incidentna %i",x,z);
              output(DEPTH,OUT);
              return 1;
            }
        }
  }
return 0;
}
```

Zapis jedne od aksioma u C verziji dokazivača EUKLID

```
int prove()
{
l1:  if (contradiction()) return 1;
l2:  if (proved()) return 1;
l3:  if (adt()) goto l1;
l4:  if (axn()) goto l1;
l5:  if (asume()) return 1;
l6:  if (axb()) return 1;
l7:  if (axp()) goto l1;
l8:  if (axsp()) goto l1;
l9:  if (MoveSent()) goto l1;
return 0;
}
```

Ključna funkcija u verziji dokazivača EUKLID na programskom jeziku C

Program se poziva komandom oblika:

```
> ce <ime_datoteke> [-f|-s|-n]
```

gde `<ime_datoteke>` označava ime ulazne ASCII datoteke koja sadrži formulaciju teoreme; opcija `-f` koristi se za ispis dokaza samo u datoteku `dokaz`, `-s` za ispis dokaza samo na ekran, a opcija `-n` za ivođenje dokaza bez ispisa. Ukoliko se program pozove bez ovih parametara ispis dokaza vrši se i na ekran i u datoteku `dokaz`. Ulazna datoteka ima strogo definisanu formu. Pre skupa premisa navodi se reč `premise`, a pre samog tvrđenja koje treba dokazati reč `teorema`. Nove konstante koje se javljaju u formulaciji teoreme označavaju se redom prirodnim brojevima. Promenljive koje su vezane egzistencijalnim kvantorom u formulaciji teoreme označavaju se redom negativnim celim brojevima. (Dokazivač za tako označene promenljive pokušava da napravi unifikaciju sa nekim od uvedenih geometrijskih objekata takvih da za njih važi tvrđenje teoreme.) Tako npr. za dokaz teoreme

Postoji ravan kojoj su incidentne dve prave koje se seku.

tj.

$$\forall x \forall y \exists z(\mathcal{L}(x) \wedge \mathcal{L}(y) \wedge x \neq y \wedge seku\_se(x,y) \Rightarrow \mathcal{P}(z) \wedge \mathcal{I}(x,z) \wedge \mathcal{I}(y,z))$$

dovoljno je dokazati (v.poglavlje 2.2.1) da važi:

$$\Gamma, \mathcal{L}(a), \mathcal{L}(b), a \neq b, seku\_se(a,b) \overset{E}{\vdash} \exists z(\mathcal{P}(z) \wedge \mathcal{I}(x,z) \wedge \mathcal{I}(y,z)),$$

pa odgovarajuća ulazna datoteka za dokazivač ima sledeći sadržaj:

```
premise
prava(1)
prava(2)
ne_identicno(1,2)
seku_se(1,2)
teorema
ravan(-1)
incidentno(1,-1)
incidentno(2,-1)
```

U dodatku je navedeno nekoliko dokaza generisanih od strane C verzije dokazivača EUKLID. Dokazi su generisani na računaru PC 386DX (40MHz).

5

DODATAK A: Geometrijski aksiomatski sistemi

David Hilbert: *Osnovi geometrije* (1899)

Za postupno izgrađivanje geometrije - isto kao i aritmetike - potreban je samo mali broj prostih osnovnih stavova. Ovi osnovni stavovi nazivaju se "aksiomama" geometrije.

Definicija. Mi zamišljamo tri različita sistema stvari: stvari prvog sistema nazivamo *tačkama* i označavamo ih sa $A, B, C, \ldots$; stvari drugog sistema nazivamo *pravama* i označavamo ih sa $a, b, c, \ldots$; stvari trećeg sistema nazivamo *ravnima* i oznaccavamo ih sa $\alpha, \beta, \gamma, \ldots$; tačke se nazivaju i *elementima linearne geometrije*, tačke i prave se nazivaju *elementima ravne geometrije*. a tačke, prave i ravni nazivaju se *elementima prostorne geometrije* ili *elementima prostora.*

Mi zamišljamo tačke, prave i ravni u izvesnim međusobnim odnosima i označavamo ove odnose rečima "ležati", "između", "podudarno", "paralelno", "neprekidno"; tačan i za matematičke svrhe potpun opis ovih odnosa postiže se pomoću *aksioma geometrije.*

Aksiome veze

I_1. Za dve tačke A, B postoji uvek prava a koja pripada svakoj od ovih dveju tačaka.

I_2. Za dve tačke A, B ne postoji više od jedne prave koja bi pripadala svakoj od dveju tačaka A, B.

(Ovde, kao i u daljim izlaganjima, pod dvema, trima,... tačkama odnosno pravama, ravnima uvek se podrazumevaju *različite* tačke, odnosno prave, ravni.

Umesto "pripadati" upotrebljavaćemo i druge načine izražavanja, npr. *prava a prolazi kroz tačke A i B, prava a vezuje A i B* ili *vezuje A sa B, A leži na a, A je tačka prave a, postoji taka A na a* itd. Ako tačka A leži na pravoj a i osim toga, na drugoj pravoj b, upotrebićemo takođe izraze: *prave a i b se seku u tački A, imaju tačku A zajedničku* itd.

I_3. Na pravoj postoje uvek najmanje dve tačke. Postoje najmanje tri tačke koje ne leže na jednoj pravoj.

I_4. Ma za koje tri tačke A, B, C koje ne leže na istoj pravoj, postoji uvek ravan α koje pripada svakoj od ove tri tačke A, B, C. Za svaku ravan uvek postoji tačka koja joj pripada.

(Mi ćemo upotrebljavati i izraze: *A leži u α; A je tačka ravni α* itd.)

I_5. Ma za koje tri tačke A, B, C koje ne leže na istoj pravoj, ne postoji više od jedne ravni koja pripada svakoj od ovih triju tačke A, B, C.

I_6. Ako dve tačke A, B prave a leže u ravni α, onda svaka tačka prave a leži u ravni α.

(U ovom slučaju kažemo *prava a leži u ravni α* itd.)

I_7. Ako dve ravni α, β imaju zajedničku tačku A, onda one imaju najmanje još jednu zajedničku tačku B.

I_8. Postoje najmanje četiri tačke koje ne leže u jednoj ravni.

Aksiome rasporeda

Definicija. Tačke neke prave stoje u isvesnim međusobnim odnosima. Za opis ovih odnosa služimo se naročito rečju "između".

II_1. Ako tačka B leži između tačaka A i C, onda su A, B, C tri različite tačke prave i B leži takođe između C i A.

II_2. Za dve tačke A i C uvek postoji najmanje jedna tačka B na pravoj AB, tako da C leži između A i B.

II_3. Od ma kojih triju tačaka prave ne postoji više od jedne koja leži između one druge dve.

II_4. Neka su A, B, C tri tačke koje ne leže na jednoj pravoj i neka je a prava u ravni ABC koja ne prolazi ni kroz jednu od tih tačaka A, B, C: ako tada prava a prolazi kroz jednu od tačaka duži AB, ona mora prolaziti kroz jednu od tačaka duži AC ili kroz jednu od tačaka duži BC.

Aksiome podudarnosti

Definicija. Duži stoje u izvesnim odnosima među sobom, za čije nam označavanje služe reči *podudarno* (*kongruentno*) ili *jednako*.

III_1. Ako su A, B dve tačke na pravoj a i ako je, dalje, A' tačka na istoj ili na drugoj pravoj a', onda se može uvek naći takva tačka B' prave a' na datoj strani od tačke A' da duž AB bude podudarna ili jednaka duži $A'B'$, što ćemo označiti na sledeći način:

$$AB \equiv A'B'.$$

Duž je bila definisan prosto kao sistem dveju tačaka i označena je sa AB ili BA. Poredak ovih tačaka nije u definiciji uzet u obzir; zato formule

$$AB \equiv A'B', AB \equiv B'A', BA \equiv A'B', BA \equiv B'A'$$

imaju isto značenje

III_2. Ako su duži $A'B'$ i $A''B''$ podudarne jednoj istoj duži AB, biće i duž $A'B'$ podudarna duži $A''B''$, ili kratko: ako su dve duži podudarne trećoj, podudarne su i među sobom.

III_3. Neka su AB i BC dve duži na pravoj a bez zajedničkih tačaka i neka su dalje $A'B'$ i $B'C'$ dve duži na istoj pravoj a ili na nekoj drugoj pravoj a' koje isto tako nemaju zajedničkih tačaka; ako je tada

$$AB \equiv A'B' \text{ i } BC \equiv B'C',$$

biće uvek i

$$AC \equiv A'C'.$$

Definicija. Uglovi stoje u izvesnim međusobnim odnosima za čije nam označavanje služe reči *podudarno* (*kongruentno*) ili *jednako*.

III_4. Neka je dat ugao $\angle(h,k)$ u ravni α i prava a' u ravni α', ako i određena stran ravni α' prema pravoj a'. Neka h' označava polupravu prave a' koja polazi iz tačke O'; onda u ravni α' postoji jedna i samo jedna poluprava k' tako da je ugao $\angle(h,k)$ podudaran ili jednak uglu $\angle(h',k')$ i u isto vreme sve unutrašnje tačke ugla $\angle(h',k')$ nalaze se na datoj strani od prave a', što ćemo označiti na ovaj način

$$\angle(h,k) \equiv \angle(h',k').$$

Svaki je ugao podudaran samom sebi, tj. uvek je

$$\angle(h,k) \equiv \angle(h,k)$$

III_5. Ako za dva trougla ABC i $A'B'C'$ važe podudarnosti

$$AB \equiv A'B', AC \equiv A'C', \angle BAC \equiv \angle B'A'C',$$

onda uvek važi i podudarnost

$$\angle ABC \equiv \angle A'B'C'.$$

(III_6.[1] Ako su dva ugla podudarna trećem, podudarna su i među sobom.)

Aksioma paralelnih

IV (Euklidova aksioma). Neka je a proizvoljna prava i A tačka van a: tada postoji u ravni određenoj pravom a i tačkom A najviše jedna prava koja prolazi kroz A i ne preseca a.

Definicija. Ako je M neka proizvoljna tačka u ravni α, onda se ukupnost svih onih tačaka A u ravni α za koje su duži MA jedna drugoj kongruentne, naziva *krugom*; tačka M se naziva

[1] Ova aksioma postojala je samo u prvom izdanju Hilbertove knjige; kako se uvidelo da ona može biti dokazana korišćenjem preostalih aksioma, u narednim izdanjima nije bila deo aksiomatskog sistema.

središte kruga.

Aksiome neprekidnosti

V_1 (Aksioma merenja ili Arhimedova aksioma). Ako su AB i CD ma koje dve duži, onda postoji neki takav broj n, da kad se duž CDprenese n puta od A jedno za drugom po polupravoj koja prolazi kroz tačku B prelazi se preko tačke B.

V_2 (Aksioma linearne potpunosti). Sistem tačaka neke prave sa svojim relacijama rasporeda i kongruencije ne može se tako proširiti, da ostanu očuvane relacije koje postoje između prethodnih elemenata, kao i osnovne osobine linearnog rasporeda i kongruencije koje proističu iz aksioma $I - III$ i aksiome V_1.

Alfred Tarski: *Šta je elementarna geometrija ?* (1969)

Elementarna geometrija je onaj deo euklidske geometrije koji može biti formulisan i dokazan bez korišćenja teorije skupova. Preciznije, elementarna geometrija je teorija sa standardnom formalizacijom. Ona je formalizovana u okviru elementarne logike, tj. predikatskog računa prvog reda. Sve promenljive $x, y, z...$ koje se pojavljuju u ovoj teoriji se odnose na elemente jednog fiksnog skupa; elemente tog skupa zovemo *tačkama*, a sam skup *prostorom*. Logičke konstante teorije su:

(i) simbol negacije $\neg$, simbol implikacije $\rightarrow$, simbol disjunkcije $\vee$, simbol konjunkcije $\wedge$;

(ii) kvantifikatori - univerzalni $\forall$ i egzistencijalni $\exists$;

(iii) dva specijalna binarna predikata - simbol jednakosti $=$ i simbol nejednakosti $\neq$;

Kao nelogičke konstante (osnovne simbole teorije) koristimo ternarni predikat β koji označava relaciju *između* i kvaternarni predikat δ koji označava relaciju *podudarnosti*. Formulu $\beta(xyz)$ čitamo *y leži između x i y*, a $\delta(xyzu)$ čitamo *x je jednako udaljen od y kao z od u*. (Kako ne koristi skupove, ovako zasnovana teorija ne pokriva geometrijske figure, klase figure i sl. Ipak, u njoj je moguće formulisati sva tvrđenja elementarne geometrije koja se odnose na specijalne klase figura (prave, krugove, duži, trouglove, poligone sa fiksnim brojem temena itd.))

Aksiome elementarne geometrije ravni su:

A1 Aksioma jednakosti za relaciju između

$\forall xy[\beta(xyx) \rightarrow (x = y)]$

A2 Aksioma tranzitivnosti za relaciju između

$\forall xyzu[\beta(yzu) \wedge \beta(yzu) \rightarrow \beta(xyz)]$

A3 Aksioma veze za relaciju između

$\forall xyzu[\beta(xyz) \wedge \beta(xyu) \wedge (x \neq y) \rightarrow \beta(xzu) \vee \beta(xuz)]$

A4 Aksioma refleksivnosti za podudarnost

$\forall xy[\delta(xyyx)]$

A5 Aksioma jednakosti za podudarnost

$\forall xyz[\delta(xyzz) \to (x = y)]$

A6 Aksioma tranzitivnosti za podudarnost

$\forall xyzuvw[\delta(xyzu) \wedge \delta(xyvw) \to \delta(zuvw)]$

A7 Pašova aksioma

$\forall txyzu\exists v[\beta(xtu) \wedge \beta(yuz) \to \beta(xvy) \wedge \beta(ztv)]$

A8 Euklidova aksioma

$\forall txyzu\exists vw[\beta(xut) \wedge \beta(yuz) \wedge (x \neq y) \to b(xzv) \wedge \beta(xyw) \wedge \beta(vtw)]$

A9 Aksioma pet duži

$\forall xx'yy'zz'uu'[\delta(xyx'y') \wedge \delta(yzy'z') \wedge \delta(xux'u') \wedge \delta(yuy'u') \wedge \beta(xyz) \wedge \beta(x'y'z') \wedge (x \neq y) \to \delta(zuz'u')]$

A10 Aksioma konstrukcije duži

$\forall xyuv\exists z[\beta(xyz) \wedge \delta(yzuv)]$

A11 Akisioma donje dimenzije

$\exists xyz[\neg\beta(xyz) \wedge \neg\beta(yzx) \wedge \beta(zxy)]$

A12 Aksioma gornje dimenzije

$\forall xyzuv[\delta(xuxv) \wedge \delta(yuyv) \wedge \delta(zuzv) \wedge (u \neq v) \to \beta(xyz) \vee \beta(yzx) \vee \beta(zxy)]$

A13 Elementarne aksiome neprekidnosti

Sve rečenice oblika

$\forall vw...\{\exists z\forall xy[\phi \wedge \psi \to \beta(zxy)] \to \exists u\forall xy[\phi \wedge \psi \to \beta(xuy)]\}$

gde je ϕ bilo koja formula u kojoj se promenljive $x, v, w, ...$, ali ne i y i z pojavljuju kao slobodne, i slično ψ, sa izmenjenim ulogama za x i y.

A13' Elementarna aksioma neprekidnosti

$\forall xyzx'z'u\exists y'[\delta(uxux') \wedge \delta(uzuz') \wedge \beta(uxz) \wedge \beta(xyz) \to \delta(uyuy') \wedge \beta(x'y'z')]$

Zoran Lučić: *Euklidska i hiperbolička geometrija*

Osnovnim pojmovima geometrije smatraćemo: skup **S**, dve klase $\mathcal{L}$ i $\mathcal{P}$ njegovih podskupova, i dve relacije: tročlanu relaciju $\mathcal{B}$ i četvoročlanu relaciju $\mathcal{C}$, koje su definisane na skupu **S**.

Skup **S** zvaćemo *prostorom*, a njegove elemente *tačkama* i obeležavamo ih velikim latinskim slovima $A, B, C, \ldots$ Elemente klase $\mathcal{L}$ zvaćemo *pravama* i obeležavamo ih malim latinskim slovima $a, b, c, \ldots$ Elemente klase $\mathcal{P}$ zvaćemo *ravnima* i obeležavamo ih malim grčkim slovima $\alpha, \beta, \gamma \ldots$

Neprazne skupove tačaka zvaćemo *likovima* ili *figurama.*

Relaciju $\mathcal{B}$ zvaćemo relacijom *između* ili relacijom *poretka tačaka na pravoj*, a formulu $\mathcal{B}(A, B, C)$ čitaćemo: tačka B je između tačaka A i C.

Relaciju $\mathcal{C}$ zvaćemo relacijom *podudarnosti*, a formulu $\mathcal{C}(A, B, C, D)$ čitaćemo: par tačaka (A, B) je podudaran paru tačaka (C, D). Umesto $\mathcal{C}(A, B, C, D)$ koristićemo i oznaku $(A, B) \cong$

(C, D).

Aksiome pripadanja.

Aksioma I1: Svaka prava sadrži najmanje dve razne tačke.

Aksioma I2: Postoji najmanje jedna prava koja sadrži dve tačke.

Aksioma I3: Postoji najviše jedna prava koja sadrži dve razne tačke.

Aksioma I4: Svaka ravan sadrži najmanje tri nekolinearne tačke.

Aksioma I5: Postoji najmanje jedna ravan koja sadrži tri tačke.

Aksioma I6: Postoji najviše jedna ravan koja sadrži tri nekolinearne tačke.

Aksioma I7: Ako dve razne tačke neke prave pripadaju jednoj ravni onda svaka tačka te prave pripada istoj ravni.

Aksioma I8: Ako dve razne ravni imaju jednu zajedničku tačku onda one imaju najmanje još jednu zajedničku tačku.

Aksioma I9: Postoje četiri nekoplanarne tačke.

Aksiome rasporeda.

Aksioma II1: Ako je $\mathcal{B}(A, B, C)$ tada su A, B, C tri razne kolinearne tačke.

Aksioma II2: Ako je $\mathcal{B}(A, B, C)$ tada je $\mathcal{B}(C, B, A)$.

Aksioma II3: Ako je $\mathcal{B}(A, B, C)$ tada nije $\mathcal{B}(A, C, B)$.

Aksioma II4: Ako su A i B dve razne tačke tada postoji tačka C takva da je $\mathcal{B}(A, B, C)$.

Aksioma II5: Ako su A, B, C tri razne kolinearne tačke tada je $\mathcal{B}(A, B, C)$ ili $\mathcal{B}(B, C, A)$ ili $\mathcal{B}(C, A, B)$.

Aksioma II6: Ako su A, B, C tri nekolinearne tačke i p prava koja pripada ravni ABC, ne sadrži tačku A i seče pravu BC u tački P takvoj da je $\mathcal{B}(B, P, C)$, tada prava p seče pravu CA u tački Q takvoj da je $\mathcal{B}(C, Q, A)$ ili pravu AB u tački R takvoj da je $\mathcal{B}(A, R, B)$.

Aksiome podudarnosti

Aksioma III1: Ako su A, B, C, D tačke takve da je $(A, B) \cong (C, D)$ i $A = B$, tada je $C = D$.

Aksioma III2: Ako su A i B bilo koje dve tačke tada je $(A, B) \cong (B, A)$.

Aksioma III3: Ako su A, B, C, D, E, F tačke takve da je $(A, B) \cong (C, D)$ i, uz to, $(A, B) \cong (E, F)$ tada je $(C, D) \cong (E, F)$.

Aksioma III4: Ako su C i C' tačke dveju otvorenih duži, AB i $A'B'$, takve da je $(A, C) \cong (A', C')$ i $(B, C) \cong (B', C')$ tada je i $(A, B) \cong (A', B')$.

Aksioma III5: Ako su A i B dve razne tačke i C teme neke poluprave tada na toj polupravoj postoji tačka D takva da je $(A, B) \cong (C, D)$.

Aksioma III6: Ako su A, B, C tri nekolinearne tačke i A', B' tačke ruba neke poluravni takve da je $(A, B) \cong (A', B')$ tada u toj poluravni postoji jedinstvena tačka C' takva da je $(A, C) \cong (A', C')$ i $(B, C) \cong (B', C')$.

Aksioma III7: Ako su A, B, C i A', B', C' dve trojke nekolinearnih tačaka i D i D' tačke polupravih BC i $B'C'$ takve da je $(A, B) \cong (A', B')$, $(B, C) \cong (B', C')$, $(C, A) \cong (C', A')$ i

$(B, D) \cong (B', D')$ tada je i $(A, D) \cong (A', D')$.

Aksiome neprekidnosti

Aksioma IV 1 (Arhimed-Eudoksova aksioma): Ako su AB i CD bilo koje dve duži tada na polupravoj AB postoji konačan niz tačaka $A_1, A_2, \ldots, A_n$ takvih da je $\mathcal{B}(A_1, A_2, \ldots, A_n)$, pri čemu je svaka od duži $AA_1, A_1A_2, \ldots, A_{n-1}A_n$ podudarna duži CD i $\mathcal{B}(A, B, A_n)$.

Aksioma IV 2 (Kantorova aksioma): Ako je $A_1B_1, A_2B_2, \ldots, A_nB_n, \ldots$ niz zatvorenih duži neke prave, takvih da svaka od tih duži sadrži sledeću tada postoji tačka X koja pripada svakoj duži tog niza.

Aksioma paralelnosti

Aksioma V 1 (Plejferova aksioma): Postoje tačka B i prava a koja je ne sadrži takve da u njima određenoj ravni ne postoji više od jedne prava koja sadrži tačku B, a sa pravom a nema zajedničkih tačaka.

6

DODATAK B: Sistemi za izvođenje dokaza

Eliot Mendelson: Uvod u matematičku logiku, 1964.

Logičke aksiome:

(1) $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A})$
(2) $(\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C}))$
(3) $(\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \Rightarrow ((\neg\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{B})$
(4) $\forall x_i \mathcal{A}(x_i) \Rightarrow \mathcal{A}(t)$, ako je $\mathcal{A}(x_i)$ dobro formirana formula predikatskog računa i t je term slobodan za x_i u $\mathcal{A}(x_i)$.
(5) $\forall x_i(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \forall x_i \mathcal{B})$, ako je $\mathcal{A}$ dobro formirana formula predikatskog računa koja ne sadrži slobodna pojavljivanja promenljive x_i.

Pravila izvođenja:

(i) Modus ponens: $\mathcal{B}$ sledi iz $\mathcal{A}$ i $\mathcal{A} \Rightarrow \mathcal{B}$.
(ii) Generalizacija: $\forall x_i \mathcal{A}$ sledi iz $\mathcal{A}$.

Logički veznici $\wedge$, $\vee$ i $\Leftrightarrow$ uvode se definicijama:

(D1) $(\mathcal{A} \wedge \mathcal{B})$ za $\neg(\mathcal{A} \Rightarrow \neg\mathcal{B})$
(D2) $(\mathcal{A} \vee \mathcal{B})$ za $(\neg\mathcal{A}) \Rightarrow \neg\mathcal{B}$
(D3) $(\mathcal{A} \Leftrightarrow \mathcal{B})$ za $(\mathcal{A} \Rightarrow \mathcal{B}) \wedge (\mathcal{B} \Rightarrow \mathcal{A})$

Gerhard Gencen: Istraživanja u logičkoj dedukciji, 1935.

$$\wedge - I: \quad \frac{A \qquad B}{A \wedge B}$$

$$\wedge - E: \quad \frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B}$$

$$\vee - I: \quad \frac{A}{A \vee B} \qquad \frac{B}{A \vee B}$$

$$\vee - E: \quad \frac{A \vee B \qquad \begin{matrix}[A]\\ C\end{matrix} \qquad \begin{matrix}[B]\\ C\end{matrix}}{C}$$

$$\forall - I: \quad \frac{F}{\forall c\, F}$$

$$\forall - E: \quad \frac{\forall x\, F}{F\{x|t\}}$$

$$\exists - I: \quad \frac{F\{x|t\}}{\exists x\, F}$$

$$\exists - E: \quad \frac{\exists c F \qquad \begin{matrix}[F]\\ C\end{matrix}}{C}$$

$$\rightarrow - I: \quad \frac{\begin{matrix}[A]\\ B\end{matrix}}{A \rightarrow B}$$

$$\rightarrow - E: \quad \frac{A \qquad A \rightarrow B}{B}$$

$$\neg - I: \quad \frac{\begin{matrix}[A]\\ F\end{matrix}}{\neg A}$$

$$\neg - E: \quad \frac{A \qquad \neg A}{F} \qquad \frac{F}{D}$$

U sistem izvođenja za klasičnu logiku ulazi i logička aksioma:

$$A \vee \neg A.$$

7

DODATAK C: Primeri

PRIMERI

Primer 1

Postoji ravan kojoj su incidentne dve prave koje se seku.

```
premise
prava(1)
prava(2)
seku_se(1,2)
ne_identicno(1,2)

teorema
ravan(-1)
incidentno(1,-1)
incidentno(2,-1)

Dokaz:

Posto se 1 i 2 seku, one imaju zajednicku tacku (oznacimo je sa 5)
Na osnovu aksiome 1.1, prava 1 pored tacke 5 sadrzi (bar) jos jednu tacku
(oznacimo je sa 8)
    Pretpostavimo da tacka 8 pripada pravoj 2
    Na osnovu aksiome 1.3, posto prave 1 i 2 imaju zajednicke dve razlicite
tacke (tacke 5 i 8) one su identicne
    Kontradikcija (equal(1,2))
    Pretpostavimo da tacka 8 ne pripada pravoj 2
    Na osnovu aksiome 1.1, prava 2 pored tacke 5 sadrzi (bar) jos jednu tacku
(oznacimo je sa 14)
    Posto tacke 5 i 14 pripadaju pravoj 2, a tacka 8 ne, one su nekolinearne
      Pretpostavimo da su tacke 8 i 14 identicne
      Kontradikcija (colin(5,14,8))
```

```
        Pretpostavimo da tacke 8 i 14 nisu identicne
          Pretpostavimo da tacka 14 pripada pravoj 1
          Kontradikcija (colin(5,14,8))
          Pretpostavimo da tacka 14 ne pripada pravoj 1
          Na osnovu aksiome 1.2, postoji prava koja sadrzi tacke 8 i 14
(oznacimo je sa 22)
          Posto i 1 i 22 sadrze tacku 8 one se seku
          Posto i 2 i 22 sadrze tacku 14 one se seku
            Pretpostavimo da su prave 1 i 22 identicne
            Posto 5 pripada 1 i 1 i 22 su identicne, sledi da 5 pripada 22
            Kontradikcija (colin(5,14,8))
            Pretpostavimo da prave 1 i 22 nisu identicne
              Pretpostavimo da su prave 2 i 22 identicne
              Posto 5 pripada 2 i 2 i 22 su identicne, sledi da 5 pripada 22
              Kontradikcija (colin(5,14,8))
              Pretpostavimo da prave 2 i 22 nisu identicne
                Pretpostavimo da tacka 5 pripada pravoj 22
                Kontradikcija (colin(5,14,8))
                Pretpostavimo da tacka 5 ne pripada pravoj 22
                Na osnovu aksiome 1.5, postoji ravan koja sadrzi tacke
5, 8 i 14 (oznacimo je sa 35)
                Posto i 1 i 35 sadrze tacku 5 one se seku
                Posto i 2 i 35 sadrze tacku 5 one se seku
                Posto i 22 i 35 sadrze tacku 8 one se seku
                Na osnovu aksiome 1.7, posto ravan 35 i prava 1 imaju
zajednicke dve razlicite tacke (tacke 5 i 8) sledi da je prava 1
incidentna ravni 35
                Na osnovu aksiome 1.7, posto ravan 35 i prava 2 imaju
zajednicke dve razlicite tacke (tacke 5 i 14) sledi da je prava 2
incidentna ravni 35
                Teorema dokazana u tekucoj grani
                (objekat -1 index 35)
  Teorema dokazana
  Utroseno vreme u sekundama:  2.00
```

Primer 2

Postoji najviše jedna ravan kojoj su incidentne dve prave koje se seku.

```
premise
prava(1)
prava(2)
ravan(3)
```

```
ravan(4)
seku_se(1,2)
ne_identicno(1,2)
incidentno(1,3)
incidentno(2,3)
incidentno(1,4)
incidentno(2,4)

teorema
identicno(3,4)

Dokaz:

Posto se 1 i 2 seku, one imaju zajednicku tacku (oznacimo je sa 11)
Posto tacka 11 pripada pravoj 1 i prava 1 pripada ravni 3, sledi da tacka 11
pripada ravni 3
Posto i 1 i 3 sadrze tacku 11 one se seku
Posto i 2 i 3 sadrze tacku 11 one se seku
Posto tacka 11 pripada pravoj 1 i prava 1 pripada ravni 4, sledi da tacka 11
pripada ravni 4
Posto i 1 i 4 sadrze tacku 11 one se seku
Posto i 2 i 4 sadrze tacku 11 one se seku
Posto i 3 i 4 sadrze tacku 11 one se seku
  Pretpostavimo da su ravni 3 i 4 identicne
  Teorema dokazana u tekucoj grani
  Pretpostavimo da ravni 3 i 4 nisu identicne
  Na osnovu aksiome 1.1, prava 1 pored tacke 11 sadrzi (bar) jos jednu
tacku (oznacimo je sa 23)
  Posto tacka 23 pripada pravoj 1 i prava 1 pripada ravni 3, sledi da
tacka 23 pripada ravni 3
  Posto tacka 23 pripada pravoj 1 i prava 1 pripada ravni 4, sledi da
tacka 23 pripada ravni 4
    Pretpostavimo da tacka 23 pripada pravoj 2
    Na osnovu aksiome 1.3, posto prave 1 i 2 imaju zajednicke dve
razlicite tacke (tacke 11 i 23) one su identicne
    Kontradikcija (equal(1,2))
    Pretpostavimo da tacka 23 ne pripada pravoj 2
    Na osnovu aksiome 1.1, prava 2 pored tacke 11 sadrzi (bar) jos
jednu tacku (oznacimo je sa 31)
    Posto tacke 11 i 31 pripadaju pravoj 2, a tacka 23 ne, one su
nekolinearne
    Posto tacka 31 pripada pravoj 2 i prava 2 pripada ravni 3, sledi
da tacka 31 pripada ravni 3
```

```
      Posto tacka 31 pripada pravoj 2 i prava 2 pripada ravni 4, sledi
da tacka 31 pripada ravni 4
      Na osnovu aksiome 1.6, posto ravni 3 i 4 imaju zajednicke tri
nekolinearne tacke (tacke 11, 31 i 23) one su identicne
      Kontradikcija (equal(3,4))
   Teorema dokazana
   Utroseno vreme u sekundama:  1.00
```

Primer 3

Ako su 1, 2 i 3 tri različite tačke incidentne nekoj pravoj 4 i ne vazi B(1,2,3) ni B(1,3,2), onda važi B(2,1,3).

```
   premise
   tacka(1)
   tacka(2)
   tacka(3)
   prava(4)
   incidentno(1,4)
   incidentno(2,4)
   incidentno(3,4)
   ne_identicno(1,2)
   ne_identicno(1,3)
   ne_identicno(2,3)
   ne_b(1,2,3)
   ne_b(1,3,2)

   teorema
   b(2,1,3)

   Dokaz:

   Posto tacke 1, 2 i 3 pripadaju pravoj 4, one su kolinearne
   Na osnovu aksiome 2.5, kako su 1, 2 i 3 tri razne kolinearne tacke,
vazi B(1,2,3) ili B(2,3,1) ili B(3,1,2)
      Pretpostavimo da vazi B(1,2,3)
      Kontradikcija (bet(1,2,3))
      Pretpostavimo da vazi B(2,3,1)
      Na osnovu aksiome 2.2, posto vazi B(2,3,1), vazi i B(1,3,2)
      Kontradikcija (bet(1,3,2))
      Pretpostavimo da vazi B(3,1,2)
      Na osnovu aksiome 2.2, posto vazi B(3,1,2), vazi i B(2,1,3)
      Teorema dokazana u tekucoj grani
   Teorema dokazana
```

```
Utroseno vreme u sekundama:  1.00
```

Primer 4

Relacija podudarnosti parova tacaka je tranzitivna.

```
premise
tacka(1)
tacka(2)
tacka(3)
tacka(4)
tacka(5)
tacka(6)
podudarno(1,2,3,4)
podudarno(3,4,5,6)
teorema
podudarno(1,2,5,6)

Dokaz:
  Na osnovu aksiome 3.3, kako vazi (1,2)=(3,4) i (1,2)=(3,4), sledi da vazi i
(3,4)=(3,4).
  Na osnovu aksiome 3.3, kako vazi (3,4)=(5,6) i (3,4)=(5,6), sledi da vazi i
(5,6)=(5,6).
  Na osnovu aksiome 3.3, kako vazi (3,4)=(5,6) i (3,4)=(3,4), sledi da vazi i
(5,6)=(3,4).
  Na osnovu aksiome 3.2, vazi (1,1)=(1,1)
  Na osnovu aksiome 3.2, vazi (1,2)=(2,1)
  Na osnovu aksiome 3.3, kako vazi (1,2)=(3,4) i (1,2)=(2,1), sledi da vazi i
(3,4)=(2,1).
  Na osnovu aksiome 3.3, kako vazi (3,4)=(5,6) i (3,4)=(2,1), sledi da vazi i
(5,6)=(2,1).
  Na osnovu aksiome 3.3, kako vazi (1,2)=(2,1) i (1,2)=(3,4), sledi da vazi i
(2,1)=(3,4).
  Na osnovu aksiome 3.3, kako vazi (1,2)=(2,1) i (1,2)=(2,1), sledi da vazi i
(2,1)=(2,1).
  Na osnovu aksiome 3.3, kako vazi (3,4)=(2,1) i (3,4)=(5,6), sledi da vazi i
(2,1)=(5,6).
  Na osnovu aksiome 3.2, vazi (1,3)=(3,1)
  Na osnovu aksiome 3.3, kako vazi (1,3)=(3,1) i (1,3)=(3,1), sledi da vazi i
(3,1)=(3,1).
  Na osnovu aksiome 3.2, vazi (1,4)=(4,1)
  Na osnovu aksiome 3.3, kako vazi (1,4)=(4,1) i (1,4)=(4,1), sledi da vazi i
(4,1)=(4,1).
```

```
   Na osnovu aksiome 3.2, vazi (1,5)=(5,1)
   Na osnovu aksiome 3.3, kako vazi (1,5)=(5,1) i (1,5)=(5,1), sledi da vazi i
(5,1)=(5,1).
   Na osnovu aksiome 3.2, vazi (1,6)=(6,1)
   Na osnovu aksiome 3.3, kako vazi (1,6)=(6,1) i (1,6)=(6,1), sledi da vazi i
(6,1)=(6,1).
   Na osnovu aksiome 3.2, vazi (2,1)=(1,2)
   Na osnovu aksiome 3.3, kako vazi (2,1)=(3,4) i (2,1)=(1,2), sledi da vazi i
(3,4)=(1,2).
   Na osnovu aksiome 3.3, kako vazi (3,4)=(5,6) i (3,4)=(1,2), sledi da vazi i
(5,6)=(1,2).
   Na osnovu aksiome 3.3, kako vazi (2,1)=(1,2) i (2,1)=(5,6), sledi da vazi i
(1,2)=(5,6).
   Teorema dokazana u tekucoj grani
   Teorema dokazana
   Utroseno vreme u sekundama:  1.00
```

Primer 5

Ako su ravni 4 incidentne različite prave 1, 2 i 3 i ako se prave 1 i 2, kao i prave 2 i 3 ne seku, onda se ne seku ni prave 1 i 3.

Dokaz:

```
premise
prava(1)
prava(2)
prava(3)
ravan(4)
ne_identicno(1,2)
ne_identicno(1,3)
ne_identicno(2,3)
incidentno(1,4)
incidentno(2,4)
incidentno(3,4)
ne_seku_se(1,2)
ne_seku_se(2,3)

teorema
ne_seku_se(1,3)

Dokaz:

  Pretpostavimo da se prave 1 i 3 seku
  Posto se 1 i 3 seku, one imaju zajednicku tacku (oznacimo je sa 14)
```

```
    Posto tacka 14 pripada pravoj 1 i prava 1 pripada ravni 4, sledi da tacka
14 pripada ravni 4
    Posto i 1 i 4 sadrze tacku 14 one se seku
    Posto i 3 i 4 sadrze tacku 14 one se seku
      Pretpostavimo da tacka 14 pripada pravoj 2
      Posto i 1 i 2 sadrze tacku 14 one se seku
      Kontradikcija (intersec(1,2))
      Pretpostavimo da tacka 14 ne pripada pravoj 2
      Na osnovu aksiome 5.1, postoji najvise jedna prava koja sadrzi tacku 14,
pripada ravni 4 i sa pravom 2 nema zajednickih tacaka, pa su prave 1 i 3 identicne.
      Kontradikcija (equal(1,3))
    Pretpostavimo da se prave 1 i 3 ne seku
    Teorema dokazana u tekucoj grani
  Teorema dokazana
  Utroseno vreme u sekundama:  1.00
```

Literatura

[Bu83] ALAN BUNDY: The Computer Modeling of Mathematical Reasoning, Academic Press Inc., 1983.

[AI87] WOLFGANG BIBEL et.al: Fundamentals of Artificial Intelligence, An Advanced Course, Springer-Verlag, Berlin Heidelberg, 1987.

[Bo60] KAROL BORSUK, WANDA SZMIELEW: Foundations of Geometry, North-Holland Publishing Company, Amsterdam, 1960.

[Ch88] SHANG-CHING CHOU: Mechanical Geometry Theorem Proving, D.Reidel Publishing Company, Dordrecht, 1988.

[Eu] EUKLID: Elementi, Naučna knjiga, Beograd, 1957.

[Gel83] H.GELERNTER: Realisation of a Geometry-Proving Machine, in Automation of Reasoning, Springer-Verlag, Berlin, 1983.

[Gen] M.E.SZABO: The Collected Papers of Gerhard Gentzen, North-Holland Publishing Company, Amsterdam, 1969.

[Hi99] DAVID HILBERT: Osnovi geometrije, Naučno delo, Beograd, 1957.

[JK95a] PREDRAG JANIČIĆ, STEVAN KORDIĆ: EUKLID - the Geometry Theorems Prover, FILOMAT 9:3 (1995), Niš, 1995.

[JK95b] PREDRAG JANIČIĆ, STEVAN KORDIĆ: Jedan pristup aksiomatskom zasnivanju geometrije, 9-i Kongres matematičara Jugoslavije, Petrovac na moru, 1995.

[Lo84] DRAGOMIR LOPANDIĆ: Geometrija za III razred usmerenog obrazovanja, Naučna knjiga, Beograd, 1984.

[Lu94] ZORAN LUČIĆ: Euklidska i hiperbolička geometrija, Grafitti i Matematički fakultet, Beograd, 1994.

[Men64] ELIOT MENDELSON: Introduction to Mathematical Logic, D.Van Nostrand Company, Inc., Princeton, 1964.

[Mes65] HERBERT MESCHKOWSKI: Temelji euklidske geometrije, Školska knjiga, Zagreb, 1978.

[Mi86] ŽARKO MIJAJLOVIĆ, ZORAN MARKOVIĆ, KOSTA DOŠEN: Hilbertovi problemi i logika, Zavod za udžbenike i nastavna sredstva, Beograd, 1986.

[Mi87] ŽARKO MIJAJLOVIĆ: An Introduction to Model Theory, University of Novi Sad, Institute of Mathematics, Novi Sad, 1987.

[NSS83] A.NEWELL, J.C.SHAW, H.A.SIMON: Empirical Explorations with the Logic Theory Machine: A Case Study in Heuristics, in Automation of Reasoning 1-2, Springer-Verlag, Berlin, 1983.

[Po63] A. V. POGORELOV: Predavanja iz osnova geometrije, Zavod za izdavanje udžbenika, Beograd, 1963.

[Pr65] DAG PRAWITZ: Natural Deduction, Almqvist & Wiksell, Stockholm, Uppsala 1965.

[SW83] JORG SIEKMANN, GRAHAM WRIGHTSON eds.: Automation of Reasoning 1-2, Springer-Verlag, Berlin, 1983.

[Ta69] ALFRED TARSKI: What is Elementary Geometry ?, EVERT W. BETH eds..: The Philosophy of Mathematics, Oxford University Press, 1969.

[Ta71] ALFRED TARSKI et.al.: Undecidable Theories, North-Holland Publishing Company, Amsterdam, 1971.

Bibliografija

[Ba37] R.BALDUS: Zur Axiomatisierung der Geometrie V.Sitzungsber. Bayer. Akad.d. Wiss.math.-nat.Abt. 1937.

[Ba38] R.BALDUS: Uber nicht bewisbare und doch entbehrliche Axiome MZ 44, 1938.

[Bl77] W.W.BLEDSOE: Non-resolution theorem proving, Artificial Intelligence, 9(1), 1977.

[Ch93] C.C.CHOU, X.S.GAO, J.Z.ZHANG: Automated production of traditional proofs for constructive geometry theorems, Collection: Eighth Annual IEEE Symposium on Logic in Computer Science (Montreal, PQ, 1993), 48–56

[Fo58] H.G.FORDER: Foundations of Euclidian Geometry, New York, 1958

[Gel63] H.GELERNTER: Realization of a geometry theorem-proving machine, in Computers and Thought, McGraw Hill, 1963.

[Gen35] G.GENZEN: Undersuchungen uber das logische Schliessen, Mathem. Zeitschr. 39, 1935.

[Ha60] G.AF.HALSTROM: Om den plana geometrins axiomsystem, Nord. Mat.-Tidskr. 9, 1960.

[Hi34] DAVID HILBERT, PAUL BERNAYS: Grundlagen dr Mathematik, Springer-Verlag, Berlin, 1968; ruski prevod: Osnovanija Matematiki, Nauka, Moskva, 1979.

[Kl52] S.C.KLENNE: Introduction to Metamathematics, Amsterdam-Groningen, 1952.

[Ku80] N.KUTLAND: Computability, An Introduction to recursive function theory, Cambridge, 1980.

[Le61] H.LENZ: Grundlagen der Elementarmathematik, Berlin, 1961.

[Pa82] M.PASCH: Vorlesungen uber neueve Geometrie, Leipzig, 1882.

[Ra97] BERTRAND RUSSELL: An Essay on the Foundations of Geometry, Dover Publications, Inc., New York 1897/1956.

[Sh77] R.E.SHOSTAK: On the sup-inf method for proving presburger formulae, JACM, 24(4), 1977.

[Sh79] R.E.SHOSTAK: A practical decision procedure for arithmetic with funtion symbols, JACM, 26(2), 1979.

[Ta51] A.TARSKI: A Decision Method for Elementary Algebra and Geometry, Berkeley and Los Angeles, 1951.