# Histórias

## O paradoxo da galinha

Para usar na aula de probabilidade condicional, Teorema de Bayes.

Era uma vez uma galinha. Ela estava sossegada no galinheiro quando viu a porta da casa se abrir e sair de lá a dona do galinheiro. A galinha tomou um susto e saiu correndo se esconder, mas olhando para o que a dona fazia. Ela se aproximou do galinheiro e espalhou milho, muito milho. A galinha ainda assustada esperou a dona voltar para a casa e logo depois saiu correndo a comer o milho.

No dia seguinte, ao ver a porta da casa se abrir, a galinha saiu correndo se esconder, mas a história se repetiu e quando a dona voltou para a casa a galinha foi correndo se fartar.

No terceiro dia, a mesma coisa. E assim seguiu a história, cada dia a galinha ficava mais confiante e sempre sendo alimentada com um gostoso milho.

Lá pelo décimo dia, quando a porta de casa se abriu e a dona saiu, a galinha foi ao seu encontro toda confiante de que receberia o milho ansiado. Quando chegou perto da dona, esta a agarrou pelo pescoço, que foi torcido e cortado. A galinha foi parar na panela.

Acho que quem inventou esta história foi Bertrand Russel ou foi o seu colega de escrita, Alfred North Whitehead . A confirmar...

## A lição de casa que era difícil

Dantzig, o desenvolvedor da otimização via método simplex, quando aluno tinha dificuldade de sair da cama pela manhã cedo. Vai daí, que chegava muitas vezes atrasado para a aula. Um dia frio em que foi particularmente difícil deixar as cobertas ele se atrasou muito e quando chegou na sala encontrou 2 problemas postos no quadro negro. Pensou que era a lição de casa, já que o professor costumava deixar 2 problemas para isso e os copiou. Eram muito difíceis, mas ele, após algum tempo, os resolveu. Na próxima aula entregou-os ao professor, pedindo desculpas pela demora. O mestre não deu muita bola jogando-os na mala.

No domingo seguinte, cedo pela manhã, Dantzig levou um susto ao ver chegar na sua casa o professor de otimização. O mestre queria saber como, diabos, ele havia resolvido esses problemas. Eles não eram lição de casa e sim 2 problemas ainda em aberto, não resolvidos por ninguém.

Ali mesmo, Dantzig foi convidado a entrar no doutorado. A tese ? Não precisava se preocupar: os 2 problemas resolvidos eram a tese.

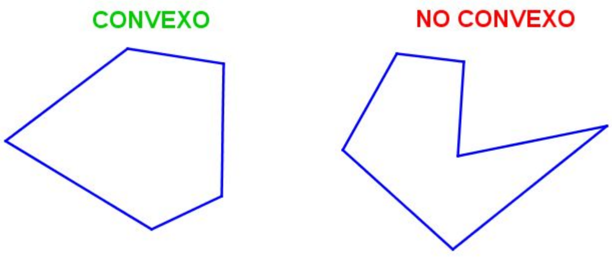
Veja `http://www.phpsimplex.com/pt/biografia_Dantzig.htm`

## O problema do final feliz

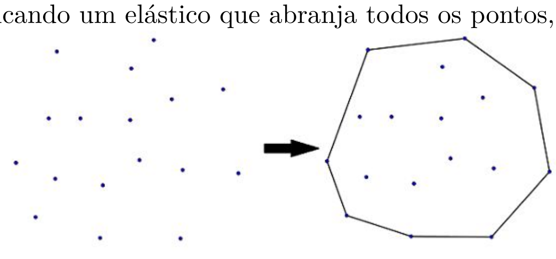
No original, nome dado por Paul Erdös: *happy ending problem*. Estamos em Budapest, Hungria em 1933. Esther Klein uma estudante de física assiste regularmente a reuniões na qual apaixonados pela matemática discutem e falam sobre ela (a matemática). Numa reunião, Esther propõe o problema:

> Dados 5 pontos no plano, tal que não haja 3 ou mais alinhados (o que se chama posição generalizada), demonstrar que existem 4 pontos que são vértices de um quadrilátero convexo.

Antes de continuar, relembre-se o conceito de convexo: um polígono é convexo quando qualquer aresta formadas por 2 pontos internos ao polígono está integralmente contida no poligono.



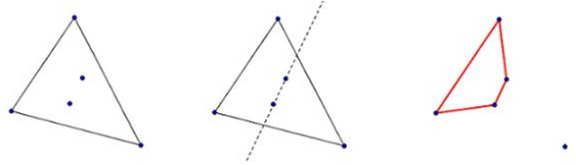

A envoltória convexa de um conjunto de pontos do plano é a intersecção de todos os conjuntos convexos que contém todos os pontos. Intuitivamente, dado um conjunto de pontos no plano, vamos cravar um prego sobre cada ponto. Esticando um elástico que abranja todos os pontos, a envoltória será o conjunto de pontos nos quais o elástico encosta.



Para resolver o problema original, vamos dividir o problema em 3 casos:

1. a envoltória convexa é um pentágono
2. a envoltória convexa é um quadrilátero
3. a envoltória convexa é um triângulo

No primeiro caso (pentágono), basta tomar 4 pontos quaisquer e temos um quadrilátero convexo, cqd.
No segundo caso, a envoltória convexa já é o quadrilátero convexo buscado, cqd.
O terceiro caso, os 2 pontos sobrantes são internos à envoltória e portanto ao triângulo. Tomando a reta que estes 2 pontos formam, dividiremos o triângulo original em 2 partes, sendo que uma contém 1 dos vértices e a outra parte contém 2 dos vértices do triângulo. Isto é certo pela condição original de não colinearidade. Tomando os 2 pontos internos e os pontos da parte que têm 2 pontos, temos os vértices do quadrilátero procurado.



Foi a própria Esther que resolveu o problema, mas a seguir ela o generalizou:

> Dado um inteiro positivo $n$ podemos encontrar o número $N(n)$ tal que para qualquer conjunto que contenha ao menos $N$ pontos seja possível selecionar $n$ deles que formem um polígono convexo ?

No caso acima, $n = 4$, a resposta é afirmativa e além disso $N(4) = 5$.

Neste ponto, dois assistentes à reunião, Paul Erdös e George Szekeres, se envolvem com o problema e em 1935 publicam um artigo conjunto com demonstrações sobre a existência desse valor $N(n)$. Como se pode ver em
`http://archive.numdam.org/article/CM_1935__2__463_0.pdf`

Mas, ficou uma pergunta sem responder: Dado um inteiro positivo $n$ qual é o menor número $N(n)$ que responde ao enunciado anterior ? Erdös e Szekeres não conseguiram responder, mas 30 anos depois, no artigo *On some extremum problems in elementary geometry* não acharam o valor exato, mas os seus limites

$$2^{n-2} + 1 \leq N(n) \leq \binom{2n-4}{n-2}$$

O problema segue em aberto, se bem que têm havido alguns progressos na questão: Já há algum tempo se acha que a cota inferior $(2^{n-2} + 1)$ é o valor de $N(n)$, mas ainda não se conseguiu demonstrar. Essa crença está reforçada pelo que se sabe dos casos $n = 5$ e $n = 6$. No caso $n = 4$ visto acima, tem-se $N = 2^{4-2} + 1 = 2^2 + 1 = 4 + 1 = 5$. Sabe-se que $N(5) = 9$ e $N(6) = 17$, mas não se conhece mais o valor exato de $N(n)$ para $n > 6$.

Finalmente, a questão de porque Erdös batizou este problema de *final feliz ?* Porque, ao estudar o problema, Esther Klein e George Szekeres acabaram se casando.

O casamento durou quase 70 anos, até que a saúde de Esther se deteriorou, afetando o próprio George. Ao que parece, ambos morreram com menos de uma hora de diferença.

Veja-se a referência em `https://www.gaussianos.com/de-como-proponer-un-problema-cambio-totalmente-la-vida-de-esther-klein/`

# Gauss de criança

O príncipe dos matemáticos Carl Gauss é certamente o maior matemático que este planeta produziu. Se você pegar uma enciclopédia de matemática, nas páginas dedicadas a Gauss, verá dezenas de contribuições todas com o seu nome. Acabei de fazer esta contagem na Enciclopédia CRC de matemática. Há 49 entradas com o nome Gauss. Impressiona mais ainda, que segundo seus biógrafos, ele tinha como mote de trabalho *pauca sed madura* fórmula latina que em bom português significa *pouco, porém maduro*. Gauss achava que uma construção matemática era como uma catedral que, antes de ser inaugurada, deveria ter todos os andaimes e auxílios da construção devidamente retirados e escondidos do público. Uma lista certamente parcial de suas criações: a geometria esférica, a teoria de grupos (aritmética dos ponteiros do relógio), a distribuição normal (a curva de gauss), a contagem dos primos, a generalização dos complexos, a solução de sistemas lineares, a interpolação polinomial, entre outros tantos.

A nossa história vai à escola fundamental onde Gauss com seus 8 anos era aluno. O professor tinha um truque para acalmar seus irriquietos alunos. Era mandar eles fazerem longas somas de números, garantindo um bom tempo de sossego. Um belo dia, precisando de um par de horas de calma, o professor mandou seus alunos somarem $1 + 2 + 3 + 4 + 5 + ... + 97 + 98 + 99 + 100$. Gauss (com 8 anos) pensou um pouco, fez uns rabiscos na lousa – já que naquele tempo não havia cadernos, o papel era muito caro – e lançou o número 5050, entregando a lousa ao professor. Não gastara mais de 2 minutos. O mestre julgou isso um atrevimento dele, mas ao final do dia, ao olhar todas as lousas, descobriu que o único que acertara a soma tinha sido Gauss.

Aqui a genialidade dele. Ao invés de sair fazendo uma soma depois da outra, como todo mundo, ele pensou sobre o problema. Sabendo que a soma é associativa, reescreveu os números a somar em 2 séries: $1 + 2 + 3 + ... + 50$ e $51 + 52 + ... + 100$. A seguir, ele inverteu a segunda série ficando $1 + 2 + 3 + ... + 50$ e $100 + 99 + 98 + ... + 51$. Agora é evidente que essas duas séries somadas vão resultar $101, 101, 101, ..., 101$. Como eram 100 números que foram divididos em 2 séries de 50, haverá 50 valores 101 na soma das séries. Daqui, o resultado procurado é $50 \times 101 = 5050$.

O danado tinha acabado de achar a fórmula da soma de uma progressão aritmetica:

$$S = \frac{(a_1 + a_n) \times n}{2}$$

. Nada mal para um piá de 8 anos, não é ?

# A aula do Knuth

TODAS AS PERGUNTAS RESPONDIDAS

Em 5 de outubro de 2001, na Universidade Técnica de Munique, Donald Knuth apresentou uma aula intitulada ”Todas as perguntas respondidas”para uma audiência de cerca de 350 pessoas. Este artigo contém uma tradução livre de alguns momentos dessa aula. Originalmente um professor de matemática, Knuth ganhou fama internacional como cientista da computação, especialmente na área de análise de algoritmos. A série seminal de 3 livros denominada The Art Of Computer Programming ainda é o que há em estudo de algoritmos, mais de 30 anos depois de sua publicação original. O longamente aguardado quarto volume está a caminho. Partes dele podem ser vistas em `www-cs-faculty.stanford.edu/~knuth/`. Knuth tem mais de 160 livros e artigos publicados e aclamados como o ”estado da arte”. Ele é o criador das linguagens TEX e METAFONT usadas para composição tipográfica, que revolucionaram a publicação de textos matemáticos no mundo, inclusive neste texto que você está lendo. A lista de prêmios e medalhas do professor Knuth é impressionante.

Knuth: Em qualquer curso que eu dou em Stanford, o último dia de aula sempre é devotado a ”todas as perguntas respondidas”. Os estudantes não precisam vir para a aula se não desejarem e os que vêm podem fazer qualquer pergunta sobre qualquer assunto exceto política, religião e exame final. Eu tirei esta idéia de Richard Feinmann (Prêmio Nobel de Física) que fazia a mesma coisa nas suas aulas na CalTech e é sempre interessante para saber as coisas que realmente interessam aos estudantes. Hoje eu responderei a qualquer pergunta sobre qualquer assunto. Sobre política e religião eu responderei ”não sei”e não há exame final para nos preocupar. Então, quem quer começar ?

Há um ligeiro mal estar no auditório e o professor Knuth diz ”Bom, já que não há perguntas...”e faz menção de ir embora. É o que basta para surgirem diversas questões.

Pergunta: Os matemáticos dizem que Deus tem o ”livro das provas”no qual estão escritas as provas de todos os teoremas. Você poderia recomendar algum algoritmo para esse livro ?

Knuth: Bonita pergunta. Eu lembro que nos anos 60, os matemáticos disseram que a ciência da computação chegaria à maturidade quando ela tivesse 1000 algoritmos profundos. Eu penso que provavelmente chegamos aos 500. Certamente há alguns algoritmos que eu penso possam ser considerados absolutamente maravilhosos e imortais, em algum sentido. Um exemplo é o algoritmo de Euclides (um algoritmo recursivo que calcula o mdc).

Pergunta: Você tem tido idéias sobre computação quântica ?

Knuth: Sim, mas eu não sei direito como esse negócio funciona. É um paradigma diferente do que eu tenho usado. Ela tem um monte de coisas em comum com a computação que eu conheço, mas é algo vagamente misterioso essa coisa de você ter todas as respostas ao final. Muitos aqui devem ter visto o filme ”Corra Lola, corra”no qual a história rola de 3 pontos de vistas diferentes. Computação quântica é parecida, o mundo vai em diferentes caminhos ao mesmo tempo e ao final escolhe-se o melhor. Eu sou razoável em computação não quântica, assim é possível que quando a computação quântica chegar, eu não seja habilidoso nela. Estou muito interessado em computação, mas porque ocorreu de eu ser bom nisso aí. Afortunadamente, eu consegui achar uma coisa na qual eu sou competente e que tem interesse para outras pessoas. Eu não desenvolvi a minha habilidade em trabalhar com algoritmos porque eu pretendia ajudar as pessoas a resolverem problemas. Quando eu era adolescente, eu tinha um jeito peculiar de pensar que me fez ser um bom programador. Mas eu não serei um bom programador em computação quântica. É outro mundo.

Pergunta: Me parece mais fácil revisar um livro do que corrigir programas. Como se pode aplicar a teoria para melhorar o software ?

Knuth: Certos erros do software são mais difíceis de corrigir do que erros em livros. De fato, eu cheguei a conclusão depois de gastar 10 anos da minha vida trabalhando no projeto TEX, que o software é ”duro”*(...the software is hard...)*. É mais difícil do que qualquer outra coisa que eu tenha feito. Nos meus livros, eu ofereço recompensas para a primeira pessoa que encontre qualquer erro, e eu devo dizer que tenho assinado mais cheques para alemães do que para cidadãos de qualquer outro país (a palestra era na Alemanha). Eu penso que deixar os usuários reportarem erros é uma técnica importante que poderia ser usada pela indústria de software. A Microsoft poderia dizer ”você obterá um cheque de Bill Gates cada vez que você achar um erro”.

Pergunta: Você tem um grande interesse em quebra-cabeças, incluindo a Torre de Hanoi em mais do que 3 pinos. Qual a melhor (menor) solução para este problema ?

Knuth: Todos aqui conhecem o problema da Torre de Hanoi ? Há 3 pinos e nestes diversos discos colocados. Os discos estão ordenados, o maior abaixo e o menor acima da pilha. A pilha toda deve ser movida, um disco de cada vez e não podendo colocar um disco grande sobre um disco menor. Há um pino auxiliar para ajudar na mudança. Henry Dudeney inventou a idéia de generalizar o problema para mais do que 3 pinos, e a questão de encontrar o menor caminho para mover a torre com 4 pinos, tem sido uma questão aberta por mais de 100 anos. Outro problema famoso é a não menos famosa Conjectura de Goldbach (todo inteiro par é a soma de 2 primos ímpares). Hoje eu penso que este problema nunca será resolvido (a prova ou a negação da conjectura). Este pode ser um dos teoremas indemonstráveis que Gödel mostrou existirem. Quanto ao problema da Torre com 4 pinos, eu cheguei a conclusão de que nunca seria capaz de resolvê-lo e eu parei de trabalhar nele em 1972. Mas antes, gastei uma boa semana trabalhando duro nele.

Pergunta: Quais são os 5 problemas mais importantes na computação ?

Knuth: Eu não gosto desse negócio das ”10 mais”(top ten) . É dos 10 de baixo (bottom ten) que eu estou interessado. Eu penso que a gente deve ir para as coisas pequenas, as pedras que farão a parede.

Pergunta: Você gastou uma grande parte de sua vida em tipografia matemática. Como avalia o impacto do seu trabalho ?

Knuth: Eu estou muito feliz porque o meu trabalho é de domínio público e torna possível as pessoas de qualquer plataforma se comunicarem pela Internet. Há duas semanas atrás eu ouvi os projetos dos jornais online da Sociedade Européia de Matemáticos. Tais coisas seriam impossíveis sem o software aberto que acabou resultando do meu trabalho. Assim, eu fico deliciado por ajudar o progresso da ciência. Eu gosto de ver livros que tem um visual bom. Antes de eu começar meu trabalho com o TEX, os livros de matemática tinham visual ruim e pioravam de ano a ano. Dava um bocado de trabalho e as pessoas que poderiam fazer algo não estavam interessadas em textos matemáticos. Eu nunca esperei que TEX se transformasse no padrão mundial de publicações matemáticas

Pergunta: Você mandou cheques para pessoas que apontaram erros nos seus livros. Eu nunca ouvi falar que qualquer dessas pessoas descontassem um único cheque. Você tem idéia de quanto dinheiro perderia se essas pessoas repentinamente sacassem o dinheiro ?

Knuth: Existe um homem que mora perto de Frankfurt que provavelmente teria mais de 1000 US$ se descontasse todos os cheques que mandei a ele. Existe um em Los Gatos, Califórnia, que eu nunca encontrei que desconta um cheque de US $ 2,56 por mês e que deve ter cheques para vários anos ainda. Devo ter enviado mais de 2000 cheques com valor médio de US$ 8,00 por cheque. Ainda que todos eles ressolvam sacar, eu ficarei no lucro: meus livros terão ficado melhores.

(Obs: no mundo da informática, ter um cheque de Knuth, devidamente emoldurado e pendurado na parede do escritório, é como ter recebido um grande prêmio. É uma honraria, daí que ninguém os desconta).

O texto original da aula pode ser encontrado em `http://www.ams.org/notices/200203/fea-knuth.pdf`

# Mulheres e a matemática

As mulheres e a matemática ou a história de Sophie German

Através dos séculos as mulheres tem sido desencorajadas de estudar matemática. Apesar das dificuldades houve diversas que se sobressaíram em seus campos. A nossa ciência (a informática) tem a ”sua”mulher: Lady Ada, filha do poeta Byron. Trabalhando anos a fio com Charles Babbage, Ada escreveu o que viriam a ser os primeiros programas de computador da história. Isso em pleno século XIX, muito tempo antes de existir o primeiro computador. Hoje ela é homenageada com a linguagem ADA, em uso pelo Dod americano, entre outros.

Mas o assunto aqui é Sophie German, uma francesa, matemática da pesada, a quem se deve um importante trabalho na área da teoria de números. Há até uma família de números primos chamados Primos de German, na forma $2p + 1$, onde $p$ também é primo. Na área da física, German desenvolveu a teoria da elasticidade dos materiais.

Sophie nasceu em 1776, filha de um negociante, bem de vida, mas longe da nobreza. Nessa época a matemática estava vedada às mulheres, mas como o assunto poderia surgir em um salão social, as mulheres tinham que ser treinadas para poder falar nisso. Surgiram assim obras que pretendiam explicar a matemática para o "cérebro feminino". Teve um livro de Francesco Algaroti que explicava o trabalho de Isaac Newton para mulheres. Como se pensava que estas estavam interessadas apenas em romance, o livro é um diálogo entre uma mulher e seu namorado. O homem fala dos princípios físicos enquanto a mulher retruca com exemplos amorosos. Devia ser uma leitura chata pra burro.

Sophie se encantou pela matemática ao ler em um livro a vida de Arquimedes. Mais do que a vida, a morte de Arquimedes. Pois, já aos 70 anos, estava Arquimedes olhando uma figura geométrica desenhada na areia da praia, quando um soldado romano, participante das tropas que recém haviam invadido Siracusa, quis saber o que aquele velho estava fazendo. O velho, dirigiu-se ao soldado e fez nenhum caso da interrupção. Deve ter dito algo assim como "Não encha o ...". O soldado não se fez de rogado e meteu a espada na barriga de Arquimedes, matando-o.

Sophie pensou que se algo era tão absorvente e inebriante deveria valer a pena estudá-lo. Ela começou e em breve estava repassando os textos de Euler e Newton, escondida, antes de dormir. Quando o pai dela descobriu, passou-lhe uma carraspana, confiscando velas e agasalhos para que ela deixasse de estudar matemática, onde já se viu. Sophie reagiu escondendo uma porção de velas e enrolando-se na roupa de cama. Passava frio mas não deixava de estudar.

Em 1794 fundou-se a École Polytechnique em Paris. Templo do saber, existe até hoje, mas só tinha um problema. Era só para homens. Sophie, passou a frequentar a escola incognita, vestida de homem. Apoderou-se da identidade de um ex-aluno, Monsieur Le Blanc. A escola não sabia que Le Blanc havia deixado Paris e continuou a imprimir resumos e exercícios para ele. Sophie escrupulosamente fazia os exercícios e devolvia-os à escola.

A coisa deu zebra, quando o professor supervisor do curso, Joseph Lagrange (outro grande matemático) quis uma entrevista com Le Blanc. Como era possível que um aluno que era uma anta, pudesse de uma hora para outra apresentar resultados tão maravilhosos ? O que ele teria feito para aprender tão rápido e tão bem ? Sophie foi obrigada a revelar seu segredo e foi um atônito mas contente Lagrange que passou a instruir e orientar "a"nova aluna. Saindo do já conhecido, Sophie começou a estudar áreas inexploradas. E sentiu necessidade de recorrer a Karl Gauss (há controversias, mas este aqui bem pode "o "maior matemático de todos os tempos). Com medo de ser rejeitada por Gauss, quem foi que assinou as cartas ? Ele mesmo, M. Le Blanc.

A correspondência entre ambos ia de vento em popa, quando durante as guerras napoleônicas, o exército francês invadiu a Prússia. Sophie ficou com medo que seu guru tivesse o mesmo fim de Arquimedes, fosse morto por acaso. Falou sobre Gauss com seu amigo o general francês Pernety, que comandava os exércitos invasores. Este, impressionado pelo interesse de Sophie fez questão de visitar pessoalmente Gauss, dizendo-lhe que sua vida estava salva graças a interferência de Mademoiselle Germain. Gauss tomou um susto, quem seria essa mulher ?

Na próxima carta, o mistério se desfez: M. Le Blanc mudou de sexo de novo. Gauss respondeu com uma carta belíssima a Sophie reconhecendo muito o trabalho dela, "ainda mais por ser mulher".

Mais para o final da vida, Gauss convenceu a Universidade de Goettingen a oferecer um título honorífico a Sophie German. Seria algo inédito, nunca antes uma mulher conseguira isso1. Vencidas as barreiras, quando a universidade ia homenageá-la, um cancer a levou primeiro. Como final desta história, quando a Torre Eifel foi erguida, colocou-se uma placa com o nome de 72 cientistas franceses cujo trabalho permitira erguer aquele monumento. Sophie, cujo colaboração provavelmente foi a mais importante dos 72, não estava lá.

## O grego Diofante, os fundamentalistas de todos os credos e as autoridades certificadoras digitais

Diofante, um matemático grego bacana que viveu há uns 1800 anos, não se sabe direito, deixou um dos grandes legados na história do homem: a obra denominada Aritmética, composta de 13 volumes. Ele tratou dos números e dos problemas envolvendo números. (Hoje tais problemas, com números inteiros, são chamados, em sua homenagem, problemas Diofantinos). Da série de 13 livros apenas 6 sobreviveram à Idade das Trevas e só servem para dar um gostinho irresistível na boca, quando se imagina o que se perdeu nos outros 7. Um desses livros deu origem ao "último Teorema de Fermat"que acaba de ser provado pelo inglês Andrew Willes, e essa é outra história. Maravilhosa também, mas é outra história. Veja-se que naqueles tempos não era moleza escrever livros. A tarefa era manual e cansativa, não se podia errar, e ao final de anos de trabalho tinha-se um único exemplar. Os mais previdentes, sabedores da raridade do objeto, corriam a guardá-lo em uma biblioteca. Os demais, pareciam não se importar muito, mais de 99

Mas, menos mal, já havia bibliotecários e bibliófilos. Na cidade de Alexandria, no Egito, esses amantes dos livros construíram, organizaram, alimentaram e mantiveram a Grande Biblioteca de Alexandria. Conta-se que por mais de 8 séculos, a biblioteca brilhou tal como o farol da cidade. Seu primeiro golpe foi um ataque de Júlio Cézar contra Cleópatra em 47 (aC). No arranca-rabo, o porto foi incendiado e a biblioteca acabou pegando fogo. Cleópatra deve ter feito beicinho, tanto que Marco Antônio, outro romano, acabou atacando a cidade de Pérgamo (de pergaminho), saqueou a biblioteca de lá e levou tudo para a reconstruída Alexandria. Conta-se que cada viajante que entrava na cidade era minuciosamente revistado e se tivesse um livro com ele, imediatamente era ”convidado”a emprestar o livro aos copistas da biblioteca que só o devolviam depois que um segundo exemplar era zelosamente guardado.

Tudo teria corrido mais ou menos bem, se o bicho homem não tivesse se envolvido em mil e uma guerras e estrepolias. A primeira é devida ao bispo cristão Teófilo. Em 389 (dC), tendo recebido a ordem de destruir todos os monumentos pagãos, pôs mãos à obra. Por azar, Cleópatra montara a biblioteca em um templo dedicado ao deus Serápis: lá se foram os livros para a fogueira, de novo. Dois séculos depois, em 642, logo após a disseminação da religião de Maomé na região e considerando a decadência de Alexandria, esta foi cercada, invadida e saqueada. Dizem que após entrar na cidade, os soldados vieram perguntar ao califa Osmar, chefe da invasão, a respeito do que fazer com os livros. A resposta dele é de lascar, para não usar verbo mais forte. Teria dito se os livros dizem o mesmo que o Alcorão, são supérfluos e podem ser destruídos. E, se ao contrário, contradizem o Alcorão, aí é que devem ser eliminados da face da terra sem deixar rastro. As termas de Alexandria foram aquecidas por muitos anos com os livros que foram sendo queimados, até não restar nenhum. De novo.

Ignora-se se e quais livros foram salvos, até hoje se tem esperança que um certo dia, alguém mexendo na baú das velharias da família surja com alguma cópia de algum dos livros perdidos de Diofante. Seria um premio, provavelmente imerecido, à raça humana.

E, aqui chegamos ao ponto focal deste texto: Supondo que surgisse tal objeto, e se levantasse a inevitável controvérsia, a pergunta que fica é: Como alguém atestaria de que se trata do livro mesmo e não de um grosso embuste ? Não sou arqueólogo, mas tenho certeza de que técnicas há. Talvez a idade do papel, medida pelo Carbono 14, ou o alfabeto usado, ou o linguajar, ou a tinta, ou as referências do livro, ou tudo isso junto, certamente habilitará um bam-bam-bam do assunto a decretar: é o livro perdido que retorna, ou ao contrário é um embuste, chamem a polícia.

Agora, um corte na história e avancemos dois ou três mil anos em direção ao futuro. Supondo que ainda haja habitantes na face da terra, o que não dá para garantir com muita ênfase, vá lá que se encontre um livro perdido há 5 séculos. Como descobrir se o livro é original ou é uma tapeação? A novidade agora é que o que vai se descobrir é apenas um arquivo magnético. Aqui não há papel, não há alfabeto, não há Carbono 14, não há quase nada, exceto um arquivo digital.

Surge então uma autoridade certificadora gerando o que tem sido chamado de ”selo cronológico digital”. Trata-se de uma certificação de que certo arquivo já existia em uma determinada forma e com conteúdo certo em um instante claramente estabelecido no passado.

Dando um exemplo: suponha que eu seja um vidente e deseje fazer uma previsão de algo que eu asseguro que vai se realizar. Uma hipótese, esta a mais comum, é deixar (qualquer coisa) acontecer e depois ir aos jornais e TVs afirmando que 2 dias antes do acontecido acontecer, eu já tinha previsto tudinho, tintin por tintin. Ainda recentemente, no episódio do ataque terrorista a Nova Iorque, vimos de novo o mesmo filme. Nada de novo sob o sol, Carl Sagan no livro Bilhões e Bilhões, fala deliciosamente sobre este assunto.

Mas, imaginemos a hipótese improvável de eu ser um vidente não pilantra e não embusteiro, isto é honesto. Então:

1. Devo criar um arquivo digital (pode ser sob Word) descrevendo tudo o que desejo.

2. Aplico ao arquivo um gerador de hash. Trata-se de um utilitário que lê o arquivo original e gera um numerão binário (tipicamente 200, 300 ou até 500 bits) que é a sua autenticação. Se eu mudar um único caractere no arquivo original e submetê-lo ao mesmo processo, o numero gerado será outro completamente diferente. É por assim dizer, uma assinatura do arquivo.

3. Envio o número hash gerado a uma autoridade certificadora, que data a assinatura, criptografa o pacote usando a sua chave pública e me envia de volta um selo temporal. Note que o arquivo original não vai para a autoridade, pelo que pode permanecer secreto.

4. A qualquer momento, de posse do arquivo, do selo temporal e da confiança da sociedade na autoridade certificadora, posso provar ter escrito o arquivo antes da data confirmada pelo selo.

Note que a partir do número hash é impossível gerar o arquivo, apenas o outro sentido (do arquivo para a assinatura) é que é possível.

O selo temporal terá que ser não falsificável, e a hora usada terá que ser acima de qualquer suspeita, provavelmente um relógio atômico preciso vinculado a uma autoridade metrológica mundial, por exemplo o NIST americano (National Institute of Standards and Technology) ou o Observatório Nacional, brasileiro.

Ainda não temos este produto sendo usado em larga escala, mas enquanto aguardamos o Diofante, podem ir se acostumando com mais essa novidade do mundo digital em que vivemos.

## Seja bem vindo, Deep Blue

Originalmente escrito em 1997.

Na semana passada tivemos a eletrizante (tanta emoção quanto as melhores novelas da Globo – e sem comerciais irritantes no meio) disputa entre Gary Kasparov e Deep Blue. De um lado, um genial enxadrista no vigor da idade e a credencial inconteste de melhor jogador de xadrez vivo. Do outro lado, um computador. Todos os jornais e revistas tem descrito o Deep Blue como um imenso e especializado cérebro eletrônico, como se dizia quando eu era criança e havia a ameaça de um computador ensandecido (e provavelmente comunista) declarar guerra à espécie humana.

Aqui a meu ver reside a falácia maior de toda a questão. Pois todos falam no hardware, descrevem como ele faz 200.000 comparações de jogadas por segundo, de quantos processadores especializados ele tem e por aí vai. Nem uma palavra sobre o software, esse sim, ouro puro, resultado do que de melhor pode a espécie humana produzir em termos de formalismo, concisão e rigor científicos. Aliás, de nada vale poder analisar 200.000 possibilidades por segundo. Há um episódio verídico que ilustra bem esse fato. Certa vez perguntaram a Ricardo Reti (um campeão mundial, grande jogador, exímio na arte de aprontar verdadeiras arapucas nas quais o infeliz oponente era atraído achando que fazia grande negócio...), quantos lances ele precisava analisar para jogar bem. Sua resposta é deliciosa: apenas um. O certo!

Há uma explicação para o fato: o hardware é produto comercial, trabalho coletivo, para o qual convergem programas, enfoques e estudos, é mais engenharia que arte, e seu fabricante tem o maior interesse, e nesse caso todo o direito, de falar à exaustão sobre ele. Já o software... bem o software é mais produção individual, está mais para arte do que para engenharia. É resultado de muitas horas de atividade solitária. Não tem o glamour do hardware, na verdade sequer tem existência física real. É pouco mais que uma abstração. Aliás, é do nosso colega Müller, também conhecido como ”o”mestre, a antológica definição: Na dúvida entre o que é hardware e o que é software, jogue os dois para cima. O que cair na sua cabeça e causar dor, é hardware. A equipe de desenvolvimento do Deep Blue é composta por 6 pessoas, sendo sua estrela um aluno de doutorado que propôs, há vários anos atrás um algoritmo mais inteligente para jogar e vencer o xadrêz. Dessas pessoas não se fala, mas são elas que literalmente carregam o deep blue no colo. Sem elas, tal máquina era capaz de perder um jogo de damas de quem aprendeu o jogo há duas semanas.

Confesso que fiquei dividido na disputa. Horas torcia pelo deep blue, ou mais especificamente falando, pelos programadores do deep blue, esperando que mais essa barreira fosse rompida e que tivéssemos a prova inconteste de que a inteligência artificial é uma área séria da ciência, com importantes realizações em seu ativo, e o mais importante com belas promessas. Horas torcia pelo Kasparov, último defensor da humanidade frente a invasão das máquinas. Nesses momentos vía-me correndo em fuga, diante de um computador enlouquecido gritando te pego, desgraçado.

Alguns podem dizer que o xadrez é mero divertimento, coisa a toa, sem importância. Lembro-me a grande difinição do Millor Fernandes, para quem o xadrez é atividade utilíssima, sendo indicada para todas as pessoas que querem ter mais habilidade de jogar zadrez. Na verdade quem já se sentou diante de um oponente, com a responsabilidade de conduzir seu pequeno exército em direção ao rei adversário, sabe que naquele pequeno retângulo de madeira há mais estratégia, arte, sacanagem, aprontação, virtude e genialidade que em muitos outros locais mais visados e glamurosos (a Onu ou a OTAN, só para ficar nos mais famosos). É uma pena que nossas escolas, não arrumem um espacinho na sobrecarregada agenda dos alunos para incentivar o xadrez. Pois este é uma das poucas coisas que ao mesmo tempo que auxilia o treinamento do raciocínio abstrato e o desenvolvimento de estratégias sobre um conjunto pequeno e estável de regras, é divertido. A boa nova do xadrez é que a lição de casa não precisa ser chata, aborrecida e cinzenta para produzir resultados. É possível desenvolver-se divertindo-se... pensando bem acho que é por isso que as escolas ignoram solenemente o xadrez...

Para os que desprezam o xadrez, vale a lembrança de que ele já foi chamado de drosóphila melanogaster da inteligência artificial. A drosóphila, é a mosca, esse ser abjeto que nos irrita, aquela da sopa do Raul Seixas. É difícil achar que tal ser tenha alguma utilidade, mas ele é uma dádiva divina para os geneticistas. Seus cromossomos são enormes, facilmente coráveis e estudáveis. Tem um ciclo reprodutivo de 11 dias, come qualquer coisa, é barata e facilmente encontrável. Portanto qualquer cientista que estude a genética há de agradecer pela existência da mosca. Quem se interessa, ainda que de leve pela inteligência artificial, tem que ser grato pela existência do xadrez.

E, para aqueles que acham ser um jogo bobo, vamos a alguns números: Uma partida média tem cerca de 40 movimentos de cada lado. 80 no total. A cada jogada, há cerca de 25 respostas possíveis. Assim se fossemos escrever numa tabela todos os jogos de xadrez possiveis de existirem, essa tabela teria um numero bem grandinho de elementos. Vejamos: no primeiro nível, são 25 possibilidades. Cada uma delas dá origem a outras 25, o que significa 625 possibilidades no segundo lance. No terceiro, são 15.625. No quarto 390.625, no quinto, 9.765.625. Lá pelo lance 60 (na verdade, no lance 30 de cada jogador) as combinações já são 7.523.310.000.000.000.000.000 .000.000.000.000. 000.000.000.000. 000.000.000.000. 000.000.000.000.000.000.000.000. Só para comparação, estimam-se existirem ”apenas”1080 elétrons no universo. Esse número de combinações é atingido lá pela altura da jogada 55. As demais ficam por conta do lucro.

Para encerrar este artigo, fica a reflexão. É falsa a afirmativa de que o desafio foi entre homem e máquina. Foi na verdade entre o Kasparov e os 6 programadores. E, lastimo dizer ao campeão mundial, que a turma da informática levou mais essa fatura...

## O suicídio que não deu certo

Paul Wolfskehl, um industrial alemão, filho de uma família muito rica, viveu na Alemanha no final do século retrasado (o 19). Era uma família esclarecida, amante das artes e das ciências. Quando estudante, Paul estudou matemática graduando-se nesta disciplina. Não foi nenhum grande matemático, nem fêz colaborações duradouras, mas a história guarda o seu nome devido a um suicídio mal sucedido.

A história começa quando Paul apaixonou-se por uma misteriosa mulher (que devia ser casada, não se sabe), e deu encima dela durante um bom tempo. A mulher se fez de rogada, negaceou, até que um dia o Paul deu o ultimatum: como é que é isso, é namoro ou amizade ? A mulher, diante da opção, disse-lhe que não queria saber dele, que a esquecesse, ela estava em outra.

Desesperado, Paul resolveu acabar com a sua vida. Mas como industrial e homem cheio de responsabilidades (e como alemão que era), resolveu botar suas coisas em ordem antes de cometer o gesto fatal. Organizado, estimou o tempo que gastaria e marcou: mato-me na sexta feira à 1/2 noite.

Já atrasado para a carga de serviço que o esperava, arregaçou mangas e começou a trabalhar: despacho de assuntos pendentes, cartas aos amigos e parentes, instruções nas empresas, ufa que canseira. Tanto se agilizou que todas as tarefas estavam concluídas lá pelas 22h de sexta feira. Sendo metódico, jamais lhe ocorreu adiantar a ”tarefa”em duas horas: havia que esperar.

Não tendo nada melhor para fazer, foi para a sua biblioteca e começou a folhear alguns livros: caiu-lhe em mãos um livro de Ernst Kummer, outro alemão que estudara por muito tempo o célebre último teorema de Fermat.1 Demonstrar este teorema era uma obsessão, e muita gente boa já havia fracassado: Euler, Gauss, Dirichlet, Legendre, Lamé, Germain, Cauchy, e o próprio Kummer. Lendo o livro, Paul Wolfskehl começou a ficar mais e mais envolvido com o tema. Até que ele julgou achar um erro no texto de Kummer. Será que ele demonstraria o célebre teorema ? Freneticamente Wolfskehl escrevia e pensava e escrevia. Horas mais tarde, um desanimado Paul conclui que Kummer estava certo, aquela abordagem que ele usara era inconclusiva, o teorema seguia sem ser demonstrado.

Mas, tendo ouvido o piar de um passarinho, olhou pela janela e viu o sol nascendo. Passara-se a hora fatídica de meia noite e ele esquecera o suicídio. Tendo chegado até a manhã seguinte, Paul Wolfskehl concluiu que aquela mulher não era tão boa assim, no fundo era uma boa bisca e não valia a pena se suicidar por ela. Rasgou cartas e instruções e foi tomar um reforçado café da manhã.

Quando muitos anos depois, em 1908, Paul Wolfskehl morreu (de velhice) a família levou um susto: ao abrir o testamento dele, havia instruções expressas de separar 100.000 marcos da fortuna e destinar esse dinheiro como um prêmio a quem conseguisse demonstrar o teorema. Nas palavras do falecido, era o agradecimento ao teorema que lhe salvara a vida.

O prêmio foi entregue no ano retrasado a um inglês, Andrew Willes, que tendo conhecido esta historinha aos 10 anos de idade, obsecou-se pelo assunto e dedicou os 28 anos seguintes a tentar demonstrar o tal teorema. Sua demonstração, já considerada correta, tem cerca de 210 páginas de texto, não sendo portanto nem parecida com aquela que teria sido descoberta por Fermat. Será que foi um blefe ? nunca saberemos.

## O Teorema da incompletude de Gödel

Em fins do século XIX, no Congresso de Matemática de Paris, em 1900, Hilbert, renomado professor em Göttingen apresentou 23 problemas, que segundo ele estariam ocupando os matemáticos do século XX. Seu segundo problema perguntava se é possível provar que os axiomas da aritmética são consistentes, isto é, dado um número finito de passos lógicos corretos, nunca se chegará a uma contradição. Na esteira desse problema, Bertran Russell, um filósofo matemático, ou será matemático filósofo ? em 1910, começou uma série de livros *(Principia Mathematica)*, na qual, baseado nos axiomas de Peano, desenvolvia todo um programa de formalização da matemática. A tentação era saborosa: provar que lógica e matemática eram a mesma coisa. Mas, o segundo problema de Hilbert continuava em aberto. Estudos posteriores de um jovem matemático austríaco, Kurt Gödel, emigrado para os EUA, que se consubstanciaram no teorema que leva o seu nome, deram o tiro de misericórdia na pretensão. Gödel provou que num sistema lógico formal existem assertivas verdadeiras que não podem ser provadas. Foi mais um sopetão na pretensão homocêntrica do Universo (assim como fizeram Copérnico, Darwin e Freud, só para ficar nos mais evidentes). Antes de passar para o Gödel, diga-se apenas que dos 23 problemas, aproximadamente a metade ainda não tem solução (terá algum dia ?), e pior (ou melhor) a matemática se desenvolveu em centenas de direções nem sonhadas por Hilbert. Ainda bem que o trabalho final dele, terminava com a citação: Enquanto uma ciência oferece abundância de problemas, ela está viva.

Antes de entrar no tema, precisamos rever alguma coisa da lógica formal. Será o nosso jargão, por assim dizer. A Lógica remonta aos gregos (o poder de argumentação significava poder político nas democracias gregas). Sobre esta base, constrói-se a lógica matemática que a partir de Leibnitz (século XVII) começa o seu desenvolvimento. A partir daqui, chega-se ao primeiro alicerce: a lógica proposicional (aquela que só admite os valores F e V) e a lógica de primeira ordem (na qual os elementos do alfabeto são infinitos).

Sobre isto, se constrói:

- A matemática clássica, sobre a qual se constroem todas as ciências exatas.
- A computação
- Lógica modal (além de V e F temos necessariamente V ou F e possivelmente V ou F).
- Lógica temporal (aquela cujos resultados dependem do tempo).
- Lógica linear
- Lógica com mais de 2 valores (além de V e F, temos a ignorância e o contraditório: V e F juntos)
- Lógica de ordem superior

Seja um exemplo ainda dos gregos: Protágoras ensinou Euathlos a argumentar. Pelo curso, Euathlos ficou de pagar uma certa quantia. Metade no fim do curso e a outra metade quando Euathlos ganhasse a sua primeira causa. Como o pagamento da segunda metade demorasse, Protágoras processou Euathlos.

Argumentos de protágoras: Se ele ganhar, terá que me pagar (já que ele ganhou a sua primeira causa). Se ele perder, terá que me pagar, já que eu ganhei a causa contra ele.

De Euathlos: Se eu ganhar, nada terei que pagar, já que ganhei a causa. Se eu perder, nada terei que pagar, já que não ganhei ainda nenhuma causa.

Pergunta-se: quem está com a razão ??

Estudando agora o problema de Protágoras: E = Eathlos ganha o caso E1 = Eathlos ganha o seu primeiro caso P = Eathlos paga a Protágoras

Na opinião de Protágoras: $((E \rightarrow E1) \wedge (E1 \rightarrow P)) \rightarrow P$

Na opinião de Eathlos: $((E \rightarrow \sim P) \wedge (\sim E \rightarrow \sim E1) \wedge (\sim E1 \rightarrow \sim P)) \rightarrow \sim P$

Resposta correta: ambas são tautologias. Resposta jurídica (dada por um advogado que manja de lógica): O Protágoras processa o Eathlos e não comparece. Daí, processa de novo.

A lógica proposicional, busca descrever a realidade e se constrói sobre poucos conceitos, a saber 1. Suponhamos querer afirmar que Mendes joga bilhar. Isso poderia ser escrito como a proposição BilharMendes, e que obviamente teria o valor V. Outra proposição poderia ser BilharJorge, que também seria V. Já a proposição BilharCadeira é claramente F, já que nenhuma cadeira joga bilhar.

2. Suponhamos querer encadear conhecimentos, do tipo: Se está quente, choverá. Usaremos o símbolo → (lê-se se... então), e escrever-se-á: Quente → Chuva.

3. Podemos negar afirmações, do tipo: se chove, não há sol. Fica Chuva →∼ Sol.

PS: Antes de continuar, reconheça-se a fragilidade da lógica para tratar o mundo real. Não há noção de passado / presente / futuro, e nem dá pra falar do tempo de Curitiba... Mas são os defeitos de qualquer modelagem. Não há o que fazer, a não ser ir em frente.

4. São necessários 2 conectivos, o E (∧) e OU (∨), para tornar mais ricas as frases. Podemos dizer que a Fulana é rica e bonita. Ficaria: BonitezaFulana ∧ RiquezaFulana. Nesse caso, para que a assertiva completa seja verdadeira, a Fulana terá que ser rica e bonita. Já o conector ou, funciona parecido. Podemos dizer que Fulano é inteligente ou maluco. A frase em lógica seria: InteligênciaFulano ∨ MaluquiceFulano. A assertiva seria V, se qualquer uma das duas o fosse.

Até aqui, a lógica é chamada proposicional, porque se baseia em proposições claramente V ou F. Mas, isso é incompleto para descrever o mundo, senão vejamos o problema famoso:

Sócrates é homem. Todo homem é mortal, logo... Sócrates é mortal.

O problema surge ao ter que se tratar o fato de que Sócrates é uma instância de homem. A regra não se aplica só a Socrates, e sim a todos os homens. Nasce a necessidade de quantificadores, a menos que estejamos interessados em fazer uma proposição distinta para um dos homens da terra.

Lógica de Predicados: O passo seguinte, é passar da lógica de proposições para a lógica de predicados. Aqui, a proposição BilharMendes, seria escrita Bilhar(Mendes), mostrando claramente que Mendes é uma das pessoas que joga bilhar, ou Mendes tem o predicado Bilhar. Na lógica de predicados precisamos de 2 novos símbolos, chamados qualificadores. O Universal é ∀ (lê-se qualquer que seja), e o Existencial é ∃ (lê-se existe). Introduz-se aqui o conceito de variável, que pode assumir qualquer valor dentro de um domínio especificado. Eis como ficaria a frase "Quem trabalha duro ou é amigo do chefe, tem promoção"em lógica de predicados:

$\forall x$ Promoção(x) $\rightarrow TrabalhaDuro(x) \vee AmigoChefe(x)$

Ou a frase: "Todo funcionário tem um chefe"

$\forall x \exists$ y ÉChefe$(y, x)$.

Há uma distinção aqui: assertivas iniciais do problema, são chamadas axiomas, enquanto conclusões obtidas a partir das regras da lógica e dos axiomas originais, são chamados teoremas. O processo recebe o nome pomposo de Modus Ponens, que nada mais é que "Se há uma axioma E1 → E2, e há outro axioma E1, segue-se que E2 é V".

Há também outra regra de inferência chamada Modus Tolens, que diz: Se há um axioma E1 → E2, e há também ∼ E2, segue-se logicamente que ∼ E1. (Donde o simbolo → pode ser lido como se e somente se).

A demonstração de um teorema pode seguir dois caminhos. O primeiro, chamado RESOLUÇÃO, vai operando os axiomas e os teoremas até topar com o teorema que se quer provar. O segundo chamado REFUTAÇÃO, parte da negação lógica do que se quer provar e mediante as tratativas usuais chega a um ponto em que uma contradição é encontrada. Está provado o teorema original.

Cláusulas: Para que os teoremas possam ser provados, todos os axiomas e teoremas precisam estar na fórmula de cláusulas. Para conseguir isso, usam-se as seguintes regras:

1. Eliminar a implicação, lembrando que $A \rightarrow B$ pode ser escrito como $\sim A \vee B$

2. Reduzir o escopo do ∼, lembrando que

$\sim\sim A = A$

$\sim (A \vee B) = \sim A \wedge \sim B$ (e vice versa $\sim (A \wedge B) = \sim A \vee \sim B$) (Lei de DeMorgan)

Por exemplo: Supondo que P = Aluno aprovado, F = frequência acima de 75% e N = nota maior que 7. Então $P \rightarrow (F \wedge N)$. Negando P - o que seria a reprovação, fica: $\sim P \rightarrow \sim F \vee \sim N$.

$\sim \forall x P(x) = \sim P(x)$ (Não há qualquer um que seja marciano = não há marcianos)

$\sim \exists x P(x) = \forall x \sim P(x)$ (Não existe uma pessoa que seja azul = para qualquer pessoa, ela não será azul)

3. Separar as variáveis que querem dizer coisas diferentes. Como os nomes são só referências, isso não altera a cláusula, então $\forall x P(x) \vee \forall x Q(x)$ deve ser trocado para $\forall x P(x) \vee \forall y Q(y)$

4. Deslocar todos os quantificadores para a esquerda. Isso agora pode ser feito, pois não há mais confusão de nomes, graças ao passo 3.

5. Eliminar o $\exists$, graças a um truque descoberto por Skolem em 1920. Trata-se de introduzir uma função (sobre a qual nada se sabe ainda), mas que permite ir em frente. Por exemplo $\exists x$ Maluco (x), pode ser trocado por Maluco(S1), onde S1 é a função proposta, e que em tempo oportuno dirá V ou F em relação à maluquice. A propósito, o nome da função "S"é homenagem a Skolem.

6. Retirar os quantificadores. Graças às etapas anteriores, isso pode ser feito. (Acredite por enquanto, no exemplo a seguir, virá senão uma prova, pelo menos uma razoável indicação de que isso funciona).

7. Separar as cláususulas unidas por ou em cláusulas unidas por E (graças a DeMorgan).

O resultado final é uma série de cláusulas, cada uma delas unidas por E, que fica implícito.

Processo de resolução A resolução agora é tomar duas cláusulas quaisquer, que resolvidas dão origem a uma nova cláusula. Para tanto, em cada uma das cláusulas juntadas deve haver o mesmo literal ora afirmado ora negado. Esses dois se cancelam, e a cláusula resultante é o que sobrou da anulação.

Se se tentar o processo de resolução por refutação (o mais fácil), deve-se acrescentar a negação do teorema a provar.

Vamos a um exemplo: Seja uma mesa que tem 2 tijolos, um sobre o outro. O de baixo é A, e o de cima é B. Claramente pode-se afirmar que Sobre(B,A) é V, e que Sobre(A,Mesa) também é V. Queremos provar que B está encima da mesa. Ou, Acima(B,mesa).

Axiomas:

$\forall x \forall y [Sobre(x,y) \rightarrow Acima(x,y)]$

$\forall x \forall y \forall z [Acima(x,y) \wedge Acima(y,z) \rightarrow Acima(x,z)]$

Percorrendo os procedimentos acima, os axiomas ficam $\sim Sobre(u,v) \vee Acima(u,v)$

$\sim Acima(x,y) \vee \sim Acima(y,z) \vee Acima(x,z)$

Queremos provar $Acima(B, mesa)$, logo introduzimos $\sim Acima(B, mesa)$. Fica o conjunto

(1) $\sim Sobre(u,v) \vee Acima(u,v)$

(2) $\sim Acima(x,y) \vee \sim Acima(y,z) \vee Acima(x,z)$

(3) $Sobre(B,A)$

(4) $Sobre(A, mesa)$

(5) $\sim Acima(B, mesa)$

Tomando (2) e (5) fazendo $x = B$ e $z = mesa$, juntando e anulando, fica

(6) $\sim Acima(B,y) \vee \sim Acima(y, mesa)$

Tomando (1) e (6) fazendo $u = y$ e $v = mesa$, fica

(7) $\sim Sobre(y, mesa) \vee \sim Acima(B,y)$

Tomando (1) com (7) fazendo $u = B$ e $v = y$, fica

(8) $\sim Sobre(B,y) \vee \sim Sobre(y, mesa)$

Tomando (3) e (8) fazendo $y = A$

(9) $\sim Sobre(A, mesa)$

Tomando (4) e (9), ambas se anulam e o resultado é NIHIL. Logo, a assertiva negada estava correta.

Há ainda o teorema da unificação, que permite - em tempo finito - substituir literais dentro das cláusulas, (já que homem (João) e $\sim$ homem (José) não podem se anular, são coisas diferentes) devido a Kowalski em 1970. Do trabalho dele surgiu a Linguagem PROLOG.

Bom, tudo isso foi para construir o jargão. Agora vamos ao Gödel. Seu teorema se baseia em um processo de 3 etapas:

1. Estabelecer as regras pelas quais axiomas (e teoremas) podem gerar novos teoremas (é isso que eu tentei mostrar aí encima)

2. Estabelecer os axiomas da aritmética em linguagem de lógica de predicados

3. Estabelecer uma forma de numeração para os teoremas assim gerados.

Pulando a etapa 1, (já vista...(?), vamos para a etapa 2). Eis os axiomas de Peano para os números naturais. Note-se que o símbolo s denota sucessor, um conceito primitivo. O sucessor de 0 é 1, de 1 é 2, ... de n é n+1:

1. $\forall x \sim (0 = sx)$ [Não existe x tal que 0 seja seu sucessor]
2. $\forall x, y(sx = sy) \rightarrow (x = y)$ [Se 2 números tem o mesmo sucessor, são iguais]
3. $\forall x, x + 0 = x$ [0 é o elemento neutro na adição]
4. $\forall x, y, x + sy = s(x + y)$ [x somado com o sucessor de y é igual ao sucessor de x+y]
5. $\forall x, y, x \times sy = x \times y + x$ [x=2, y=5 leva a 2 × 6 = 2 × 5 + 2 = 12]
6. $\forall x, x \times 0 = 0$ [0 é o elemento absorvente na multiplicação]
7. $\forall x, x = x$ [identidade]
8. $\forall x, y, z(x = y) \rightarrow ((x = z) \rightarrow (y = z))$ [propriedade transitiva]

9. $\forall x, y(x = y) \rightarrow (A(x, x) \rightarrow A(x, y))$ [A é qualquer fórmula com 2 variáveis livres]

10. $(P(0) \wedge \forall x P(x) \rightarrow P(sx))) \rightarrow \forall x P(x)$ [Regra fundamental da indução matemática]

Com estas informações, Gödel, passou à etapa 3 do teorema, usando a tabela a seguir:

| Símbolo | Código | Símbolo | Código | Símbolo | Código |
|---|---|---|---|---|---|
| 0 | 1 | ( | 6 | $\sim$ | 11 |
| s | 2 | ) | 7 | $\wedge$ | 12 |
| + | 3 | , | 8 | $\exists$ | 13 |
| $\times$ | 4 | x | 9 | $\forall$ | 14 |
| = | 5 | 1 | 10 | $\rightarrow$ | 15 |

Note-se que só existe a variável x. Logo quando só aparece x, ele será identificado como x1. Quando aparecerem x e y, eles serão x1 e x11, e assim por diante.

Agora para cada cláusula, Gödel bolou um número, que mais tarde foi chamado ''Número de Gödel'', e que é construído da seguinte maneira. Tomam-se os primos a partir do 2. São eles: 2, 3, 5, 7, 11, 13, 17, 23, 29... Cada axioma terá seu número de Gödel calculado por um sistema de numeração onde as bases são os primos e os expoentes são o numerinho da tabela acima. Para clarear, vejamos o número de Gödel do axioma 4 de Peano:

$\forall x, yx + sy = s(x + y)$ [Escrito em linguagem matematica]
$x_1 + sx_{11} = s(x_1 + x_{11})$ [Escrito na forma de Gödel], e o número é:
$2^9.3^{10}.5^3.7^2.11^9.13^{10}.17^{10}.19^5.23^2.29^6.31^9.37^{10}.41^3.43^9.47^{10}.53^{10}.59^7$

Note-se que o numero é enorme, mas isso é de propósito. É para que, dado um número, SE ELE FOR UM NÚMERO DE GÖDEL, possa-se recuperar qual o axioma ou teorema que lhe deu origem. Basta fatorá-lo em seus componentes primos, e verificar qual o expoente de cada um dos primos. Ou seja, a relação axioma - número de Gödel é bi-unívoca.

Estamos chegando perto da prova:

Seja o predicado $PROVA(x, y, z)$, lido como $x$ é o número de Gödel da prova da fórmula Y (que tem número de Gödel y), o qual teve o inteiro z inserido dentro dela. Note-se que $PROVA(x, y, z)$ é um jeito fácil de escrever uma imensa e longa expressão onde aparecem $x_1, x_{11}$ e $x_{111}$, Essa expressão inclui muitos procedimentos, entre eles:

- dado um inteiro, fatore-o em seus fatores primos
- ache a expressão que lhe deu origem
- verifique se a expressão verifique se ela é uma fórmula
- verifique se ela esta provada

Claramente são procedimentos irrealizáveis na prática, mas em princípio, computáveis.

Vamos considerar um caso especial do predicado acima: Suponha que a fórmula Y é alimentada com seu próprio número de Gödel, e vamos tentar negar a existência de tal prova. Escreve-se $\sim \exists x PROVA(x, y, y)$
Em palavras: x é o número de Gödel da prova obtida na fórmula Y pelo número y (Número de Gödel de Y). Vamos chamar ao número de Gödel da $PROVA(x, y, y)$ de g.

Finalmente:
TEOREMA DE GÖDEL
$\sim \exists x PROVA(x, g, g)$ é verdadeiro, mas não é provável (no sentido de poder ser provado) no sistema aritmético formal.

A demonstração ocupa poucas linhas:

Suponha que $\sim \exists x PROVA(x, g, g)$ é provável (no mesmo sentido) e seja p o número de Gödel dessa prova P. Então, nós temos que $PROVA(p, g, g)$ é verdadeiro, desde que P é a prova de G, na qual foram substituídas as variáveis livres. MAS, a veracidade de $PROVA(p, g, g)$ contradiz $\sim \exists x PROVA(x, g, g)$, e daqui temos que não existe essa prova P.

Então, se tudo foi construído direitinho, a afirmação $\sim \exists x PROVA(x, g, g)$ é verdadeira e portanto não existe a $PROVA(x, g, g)$ dentro do sistema.

Em resumo: Dentro de um sistema de lógica formal existem teoremas que são indecidíveis.

Este tema está em conexão com o Paradoxo de Russel (o barbeiro da aldeia barbeia todos os homens que não se barbeiam sozinhos.) e com o argumento de Turing de que não há máquina de Turing capaz de resolver o problema de quando parar. Todos eles se baseiam na genial sacada de Cantor, chamada de corte diagonal, quando ele estudava o infinito.

Para saber mais: Matemática Moderna (Walther Fuchs); The Emperor's New Mind - Concerning Computers, Minds and Laws of Physics (Roger Penrose); The Turing Omnibus (A.K. Dewdney); Artificial Intelligence (Patrick Winston); Artificial Intelligence (Elaine Rich).