AVANTGARDE
ASSET MANAGEMENT

Avantgarde Asset Management Gestão de Recursos Ltda.
Avenida das Nações Unidas, 12399 – 7º andar
Brooklin – São Paulo – SP
CEP: 04578-000
avantgardeam.com.br
+55 11 3400-7061

Junho, 2023

Pílulas da Academia V: $P = NP?$

If $P = NP$, [...] everyone who could appreciate a symphony would be Mozart; everyone who could follow a step-by-step argument would be Gauss; everyone who could recognize a good investment strategy would be Warren Buffett.

Scott Aaronson, American Computer Scientist

O domínio dos investimentos quantitativos reside na interseção entre matemática, ciência da computação e finanças. Sem um sólido entendimento dos princípios matemáticos e das técnicas computacionais, um profissional de finanças se encontraria incapacitado de expressar efetivamente sua intuição ou implementá-la de forma eficaz e escalável. Por outro lado, um matemático ou cientista da computação sem proficiência em finanças enfrentaria desafios para transpor seu conhecimento para ideias ou estratégias de investimento.

Neste contexto, ao contrário das cartas anteriores que se concentravam mais em tópicos financeiros, esta carta aborda um dos maiores problemas ainda não resolvidos na ciência da computação: a questão de se $P = NP$ ou $P \neq NP$. Mais adiante, vamos apresentar a natureza desse problema, mas antes, para mostrar sua relevância, vale ressaltar que este é um dos sete problemas do Prêmio do Milênio, que recompensa com um milhão de dólares qualquer pessoa que consiga resolver um deles.

Os algoritmos polinomiais, identificados pelo "P" em $P = NP$, são aqueles que podem ser resolvidos em um período de tempo razoável. São denominados polinomiais porque seu tempo de execução aumenta proporcionalmente à uma função polinomial do tamanho da entrada. Isso contrasta com os algoritmos exponenciais, onde o tempo de execução aumenta exponencialmente com o tamanho da entrada, tornando-os impraticáveis para entradas muito grandes.

Para ilustrar a ideia de algoritmos polinomiais, considere que temos uma lista com n números inteiros. Podemos encontrar a posição de um número nessa lista verificando se este número está em cada uma das n entradas. Esse algoritmo apresenta uma complexidade de tempo $O(n)$, indicando que o tempo necessário para localizar a posição de um elemento específico cresce linearmente com a quantidade de elementos na lista.

Por outro lado, a classe NP engloba problemas de decisão - resposta é "sim" ou "não" - para os quais podemos verificar se a resposta é "sim" em tempo polinomial, com base em um certificador (solução candidata). Como exemplo, pense no problema de determinar se o número n possui um fator menor que k. Nesse caso, se formos apresentados com um número y menor que k, somos capazes de verificar em tempo polinomial se esse número y é um fator de n - simplesmente verificamos se o resto da divisão de n por y é zero.

Com base nessas informações, somos capazes de definir o problema em questão. Para que P seja igual a NP, é necessário que P esteja contido em NP ($P \subseteq NP$) e, simultaneamente, NP esteja contido em P ($NP \subseteq P$). Em termos simples, isso significaria que todo problema cuja solução pode ser verificada rapidamente (NP) também pode ser resolvido rapidamente (P). Se essa condição for satisfeita, ambos os conjuntos seriam equivalentes.

Avantgarde Asset Management Gestão de Recursos Ltda.
Avenida das Nações Unidas, 12399 – 7º andar
Brooklin – São Paulo – SP
CEP: 04578-000
avantgardeam.com.br
+55 11 3400-7061

De fato, $P \subseteq NP$, dado que, se conseguimos resolver um problema em tempo polinomial, também conseguimos realizar a certificação em tempo polinomial. No entanto, provar que $NP \subseteq P$ é uma tarefa significativamente mais desafiadora. Na realidade, essa questão é tão complexa que, mesmo após mais de 50 anos desde a proposição inicial desse problema, ninguém conseguiu confirmar se NP está ou não contido em P.

Neste momento, o leitor pode estar questionando a relevância de P ser igual ou diferente de NP. De fato, qual a implicação de $P = NP$ que torna esse um dos principais problemas em aberto em toda a ciência da computação? Para esclarecer isso adequadamente, precisamos introduzir outro conceito importante: os algoritmos NP-completos.

Para um algoritmo ser classificado como NP-completo, ele precisa estar em NP e ser pelo menos tão difícil quanto qualquer outro problema em NP. Essa segunda parte da definição parece beirar o absurdo. Seria o equivalente à afirmar que certas pessoas "NP-completas" são pelo menos tão inteligentes quanto qualquer outra pessoa. Seguindo essa definição, não haveria inteligências incomparáveis e não existiria uma sequência de pessoas em que cada indivíduo é sempre mais inteligente que o anterior.

De fato, esse conceito é bastante contraintuitivo, mas é onipresente em ciências da computação. Cook (1971) foi o primeiro a provar que um problema é NP-completo. Desde então, vários pesquisadores têm seguido essa linha de estudo, e hoje temos milhares de problemas comprovadamente NP-completos. Para termos uma ideia da extensão desse universo, Aloupis, et. al. (2015) mostram que até mesmo jogos populares como *Super Mario*, *Donkey Kong*, *Legend of Zelda*, *Metroid*, e *Pokemon* são NP-completos.

O interessante é que essa definição leva a um fenômeno curioso: todos os problemas NP-completos são equivalentes. Em outras palavras, os milhares de problemas NP-completos são diferentes manifestações de um único problema com múltiplas facetas, representando uma única classe de complexidade para a qual ainda não temos um completo entendimento.

Até o momento, só conhecemos algoritmos exponenciais para solucionar problemas NP-completos. No entanto, não foi possível demonstrar a inexistência de um algoritmo polinomial. Agora, se tal algoritmo polinomial existisse, isso implicaria que todos os problemas em NP podem ser resolvidos em tempo polinomial. Essa suposição levaria à conclusão de que $NP \subseteq P$ e, consequentemente, que $P = NP$.

Em outras palavras, se conseguirmos mostrar que existe um algoritmo polinomial para qualquer um dos milhares de problemas NP-completos, estaríamos demonstrando que existe um algoritmo polinomial para todos os problemas em NP. Isso pode parecer apenas uma curiosidade teórica, mas as implicações práticas seriam imensas. Como exemplo, diversos sistemas de criptografia dependem diretamente do fato de não conhecermos soluções eficientes para quebrá-los. No entanto, se $P = NP$, saberíamos que tais algoritmos existem, o que representaria um sério problema de segurança.

Como mencionado anteriormente, ainda não temos a resposta definitiva para essa pergunta. No entanto, em uma enquete realizada em 2019 com cientistas da computação, 80% dos participantes afirmaram acreditar que $P \neq NP$. Logicamente, essas crenças não são baseadas em evidências concretas, mas refletem o sentimento da comunidade acadêmica de que a igualdade $P = NP$ é muito elegante para ser verdadeira.

Atenciosamente,

Pedro Teles

AVANTGARDE
ASSET MANAGEMENT

Avantgarde Asset Management Gestão de Recursos Ltda.
Avenida das Nações Unidas, 12399 – 7º andar
Brooklin – São Paulo – SP
CEP: 04578-000
avantgardeam.com.br
+55 11 3400-7061

Avantgarde Multifatores FIA

Em junho, o fundo teve retorno de 8,78% contra 8,87% do IBX. Em 2023, o retorno acumulado do fundo é de 7,78% contra 6,59% do *benchmark*. Desde o início, o fundo tem 75,32% de retorno total contra 18,18% do IBX. Na perspectiva de risco, a volatilidade - desvio padrão anualizado - das cotas diárias do fundo, desde o início, está em 21% contra 28% do IBX. O beta, por sua vez, é de 0,65 (modelo CAPM). O alfa de Jensen resultante é de 9,33% ao ano.

As posições que mais contribuíram para o retorno do fundo foram: Odontoprev (ODPV3), Mahle Metal Leve (LEVE3), Plano & Plano Desenvolvimento (PLPL3), Marcopolo (POMO4) e Petrobras (PETR4). Por outro lado, as posições que menos contribuíram foram: Magazine Luiza (MGLU3), Salesforce (SSFO34), Mercado Libre (MELI34), São Martinho (SMTO3) e Stoneco (STOC31).

O Avantgarde Multifatores FIA entra em julho totalmente alocado em ativos de risco, com aproximadamente 90% do patrimônio alocado em ações, 9% em recibos de empresas estrangeiras negociados no Brasil (BDR) e 1% de caixa.

Avantgarde Icatu Prev 70 FIC FIM

Em junho, o fundo teve retorno de 5,51% contra 2,39% do IMA-B. Em 2023, o retorno acumulado do fundo é de 7,9% contra 11,37% do *benchmark*. Desde o início, o fundo tem 11,63% de retorno total contra 18,82% do IMA-B. Na perspectiva de risco, a volatilidade - desvio padrão anualizado - das cotas diárias do fundo, desde o início, está em 10,26% contra 5,17% do IMA-B. O fundo tem volatilidade alvo de 10% ao ano, bem próximo da volatilidade observada.

O fundo entra em julho com 68% de alocação na estratégia Multifatores de renda variável e com 31% em renda fixa.

Fatores de Risco

Os principais fatores de risco *long-only* tiveram os seguintes retornos no mês:

- Carry: 11,67%
- Low Vol: 7,81%
- Momentum: 8,33%
- Quality: 6,50%
- Value: 15,09%