科學講堂
逢星期三見報

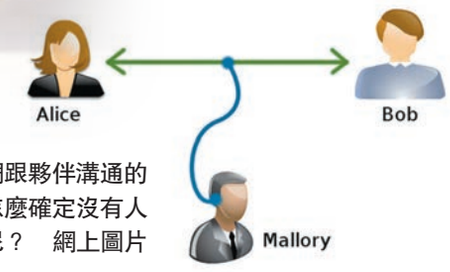
通訊雙方能迅速察覺資料是否外洩

量子密鑰技術 防止訊息被竊

大家看過班奈狄克．康柏拜區（Benedict Cumberbatch）主演的電影《解碼遊戲》（Imitation Game）嗎？電影中由他飾演的圖靈（Alan Turing）和他的夥伴同心協力，運用他們的智慧，破解二戰時期德軍使用的複雜密碼，最終成功解讀其機密軍事訊息，協助盟軍取得勝利。現今我們當然不在戰爭中，但不代表密碼跟我們風馬牛不相及：每次我們收發電子郵件，同樣經過加密及解密程序，即使他人竊取了我們的郵件，也無法理解箇中意思。從用家角度，當然希望編寫密碼的方法愈來愈難破解，我們的電子郵件才不會被人竊讀。在這方面，科技能幫助我們嗎？

▲二戰時期德軍使用的複雜密碼機。網上圖片

◀試想像量子系統是用撲克牌砌成的「紙牌屋」，如果有人進行竊聽，會改變系統導致「紙牌屋」塌下。網上圖片



▶在我們跟夥伴溝通的時候，怎麼確定沒有人在偷聽呢？ 網上圖片

謎樣訊息 外人難解讀

須知道每次編寫秘密訊息，均需要一個保密編碼方法。現時已有足夠複雜，難以破解的編碼方式。例如選擇一本書籍，然後查閱想傳達的字或字母，出現在書中哪個位置，再用數字去代表這個位置。（例如一本書的第十二頁第三行第六個字是「密」，那麼我就用1236去代表「密」字。）這樣的話，我要傳遞的訊息便變成一連串看起來毫無意義的數字，外人難以解讀。

當然真正的收件人需要懂得如何閱讀這個謎樣的訊息，因此我需要告訴對方我挑選了哪一本書。

問題來了：在我跟夥伴溝通的時候，怎能確定沒有人在偷聽呢？若偷聽者知道解密的方法，怎樣複雜的編碼方法也是浪費時間。

傳統編碼方法 未能察覺竊聽

如何解決這個問題？首先要注意的是，為安全起見，在以上提到的編碼方式下，我是不應該用同一本書去為超過一個秘密訊息編碼的，因為有心解讀的人，可能會從幾個訊息中看出關連，看到有些數字組合經常出現，因而推斷出這些可能是一些常用字（例如中文的「的」、「得」、「地」）。不重用同一本書去編碼，就免卻了這個問題了。

這樣的考慮，提醒了我們，用來編碼的書籍，本來就是應該頻繁更換的，而且跟原來要發送的秘密訊息，是兩個分開的部分。因此我們可以先將編碼用的書名告訴同伴，再注意是否被人偷聽了：如果沒有，我們當然繼續把原來的秘密訊息發送出去；如果真的有偷聽者，我們便馬上停止，稍等片刻才重試。這樣的話，我們也只是「洩露」了一些書名，並不影響原來的秘密訊息。

竊聽改變量子系統

要如何精準地發現偷聽者的存在？奇詭的量子力學為此提供了一個可能性。在量子效果不重要的情況下（比如說傳統的電流、大氣電波傳送，甚至是手寫密函），偷聽者只要夠小心，便可神不知鬼不覺地偷聽或偷看，且不着痕跡。不過，在量子力學的世界中，偷聽或偷看的行為，卻會無可避免地對這個世界造成不能忽略的影響，等於告訴大家「我偷聽/看過了！」大家可將一個量子系統想像成一個藏在盒子中、用撲克牌砌成的塔：任何想打開盒子、一窺究竟的人，將導致這個塔以某種形式崩塌，讓真正收件人在打開盒子時，發現塔子曾崩塌多過一次，自然知道有偷看者來過了。

■張文彥博士
作者簡介：香港大學土木及結構工程學士。短暫任職見習土木工程師後，決定追隨對科學的興趣，在加拿大多倫多大學取得理學士及哲學博士學位，修讀理論粒子物理。現任香港大學理學院講師，教授基礎科學及通識課程，不時參與科學普及與知識交流活動。

奧數揭秘
逢星期三見報

大數運算中的觀察

平常課程內，數字的大小許多時都只是兩三個位，若是運算過程複雜的，或是數字都比較大，往往就要求助於計算機了。不過若是能夠靈活運用一點數學知識，在一些情況下，也可以繞過計算機，直接看到答案。

問題 若$X^3=456533$，求x。

答案 先觀察等式右方數字的個位，考慮x的個位若為0，1，2，…，9，則3次方之後，只有$7^3=343$的個位是3。然後考慮x的大小。由於右方是6位數，必小於$100^3=1000000$，因此x小於100。而$70^3=343000$，$80^3=512000$，得知x在70與80之間，從而得知x為77。經驗算後得知結果屬實。

多心算穩基礎 勿依賴計算機

這題的技巧，大致上就是看個位和估算。其中看個位的部分，0至9的個位，取不同次方的時候，是會循環或不變的，比如0、1、5和6都是各次方都不變。而個位是4的話，則由$4^1=4$，$4^2=16$，$4^3=64$，得知4的各次方的個位，是在4與6之間循環，9的情況也類似。因此4和9是每2次方就循環一次。其餘的2、3、7和8，都是每4次方循環一次的。這個讀者不妨自行驗證一下。

估算的方法，也是解題中的關鍵，因為個位是3的數是很多的，若是對x的大小毫無認識，很難算出來。由等式右方的數有多少個位，來估計x是多少位數，就是解難的重點了。

估算和看個位的想法，在奧數的範圍內是簡單的，不過在這題看來，效果是很好的，可以幫助我們求出一個六位數的立方根。若是缺乏看個位的知識，單是要試出來，也是會覺得太過複雜的。

若是面對很大的數，要計算起來，現代多是用計算機的。不過若是嘗試把數字觀察一下，問一問自己能否在觀察算式之中，多少對答案的形式和大小有點概念，那樣對學數學是有好處的。

事實上有不少學生，把什麼計算都交給了計算機，即使錯得很誇張，答案差了十多倍也好，也是無法看出有問題。這樣被計算機取代了思考，最終損失的都是自己。

用計算機運算當然是易學的，若是另一方面配合課外的知識和多角度的推論，那樣兩方面計算與觀察都一致，得到的答案就令人有信心了。只有計算機計算的一邊，計完也沒有其他角度修正的，得着的信心也有限。

奧數是不能用計算機的，但它培養了學生多角度推論的能力，也豐富了學生的課外知識，這就彌補了學生單用計算機的不足，之後學生在擁有良好奧數能力之下，再配合計算機或軟件，就能夠有更精準的看法，推論也能更穩更遠，得着更大。 ■張志基

科技暢想
隔星期三見報

數據或算法誰較重要？

■人工智能在未來世界的角色愈來愈重要。 網上圖片

對於人工智能（Artificial Intelligence, AI）來說，數據和算法，哪一樣較為重要呢？這個問題目前還沒有清楚明確的答案。這數年來，有關的專家，甚至是「非專家」一直為這個疑問在爭辯，而答案取決於許多細節。

這個問題或會令人馬上聯想到機器學習（Machine Learning, ML），然而，人工智能和機器學習其實是兩回事。事實上，機器學習只是人工智能的一個子領域，需要專門的數據來訓練算法。人工智能確實包含了其他基於邏輯或規則的方法，並且不一定要像機器學習一樣需要那麼多的數據。

大多數人可能不太在乎機器學習與人工智能之間的分別，並會將兩者混合使用。而事實上，現時有很多人將人工智能用作深度學習的同義詞，它本身就是一種特殊的機器學習方法。所以筆者認為，亦可以從深度學習的角度去思考人們爭辯了數年的問題，即是：

在現代深度學習方法中，數據是否比算法更重要？

筆者的回應為亦是亦非。的確，深度學習需要非常龐大的數據，它的算法有許多參數需要調整，因此需要大量數據，以想出一些可以概括的模型。因此，從這個意義上講，大量數據是良好深度學習的關鍵。事實上，有些人曾經解釋過，像Imagenet這樣的大型公共圖像數據集的出現，與最近AI於圖像辨識的研究進展之間，正正有直接關係。

不過值得注意的是，公共數據集的存在，讓一般人亦能擁有大量數據，因而減低了數據的競爭優勢。另外，在一些算法或運算方式之中，有趣的地方是，它們有時可以被擁有數據集的人或團體「預先培訓」，然後應用至大量的使用者。在這些個案裡，人工智能往往變得不太需要數據。

以下的比喻或者會讓讀者更易明白：如果你要訓練一個將英文翻譯成西班牙語的模型，你需要做的就是收集一個龐大的數據集，並訓練模型一次，該模型本身已帶有所有訊息，因此任何能夠獲得該模型的人都不再需要原始數據；亦可以說，這些特別的算法已經包含數據的「精華」在其中。 ■洪文正

有問有答
隔星期三見報

凍土大量融化 或加速全球變暖

凍土融化會影響全球變暖嗎？若凍土中的有機碳融化，變成二氧化碳或甲烷，使大氣中的溫室氣體濃度增加，便會令全球變暖。

在寒冷的極地和高山地區，地表被大量的永久凍土所覆蓋。隨着全球氣溫不斷上升，這些凍土將會逐漸融化。我們知道融化過程是吸熱的，那凍土的融化是會使全球變暖減緩呢，還是會使氣溫升高得越來越快呢？

動植物殘體藏凍土

首先，凍土融化所吸收的熱量十分有限，並不足以對氣候造成很大影響。但是，在凍土中蘊藏許多「壞分子」—有機碳，它們有可能對氣候產生強烈的影響。自末次冰期以來，大量的動植物殘體，在凍土的季節性凍融過程中，被埋藏在凍土層中。在凍土層中，由於溫度很低，水基本上以冰的形式存在，微生物活動基本停止，使得這些有機碳得以保存在凍土中，從而脫離了與其他圈層的交換。

凍土融化 釋放「壞分子」

經過數千年的積累，這些永久凍土中含有大量的有機碳，據科學家估計相當於目前大氣中碳含量的兩倍。這些「壞分子」跟大氣中最重要的溫室氣體二氧化碳有密切的關係。當永久凍土逐漸融化時，這些「壞分子」會在微生物的幫助下，變成二氧化碳或甲烷，再跑到大氣中去，使大氣中的溫室氣體濃度增加，溫室效應增強，氣溫上升。而大氣溫度上升，又會促使凍土進一步融化，釋放更多的有機碳，如此形成惡性循環。

那麼，凍土的融化使得全球變暖加速了？實際上問題沒有那麼簡單，因為凍土融化還會產生另一種效應：融化後土壤水熱條件的改善、二氧化碳濃度的增加，以及生長季節的延長等，均有利於植物的生長，增加凍土區的初級生產力。植物的大量生長可以通過光合作用，從大氣中吸收更多的二氧化碳，從而減弱大氣溫室效應，進而減緩全球變暖。

甲烷較二氧化碳 多30倍溫室效應

如此說來，凍土的融化到底會不會加劇全球變暖，還得要看上面提到的這兩種效應哪一種更大了。目前的科學研究一般認為，凍土融化所釋放出來的碳要比生產力增加所吸收的碳多，而且當凍土融化時，其中含有的有機碳不僅能以二氧化碳的形式進入大氣，還能夠在微生物的作用下形成甲烷，甲烷的溫室效應大約是同體積二氧化碳的30倍。

總的來說，未來如果永久凍土大量融化的話，很可能會加速全球變暖。

不過到目前為止，凍土融化對大氣中溫室氣體濃度和全球氣候究竟會產生多大的影響仍然是不確定的，還有待探索。

■近年凍土融化形成的湖。 出版社供圖