Turbo 码给我们的启示

冀复生

今天 Turbo 码在通信界已经几乎无人不晓。用 Google 搜索“Turbo code”可以得到 800 多万结果。在未来的第三代移动通信中，它很可能成为编码方案的标准之一（即使不采用它，新的方案也很可能是受其启发，基于与它相似的思路而产生的类似方案），但是 Turbo 码诞生过程却有一段引人入胜的故事。

1993 年在日内瓦召开的 IEEE 通信国际会议上，两位当时名不见经传的法国电机工程师克劳德.伯劳和阿雷恩.格莱维欧克斯声称他们发明了一种编码方法，可以使信道编码效率接近香农极限。这一消息太“轰动”了，以致多数权威认为一定是计算或实验有什么错误。许多专家甚至懒得去读完这篇论文。

在数字通信领域，编码效率一直是关注的焦点。根据现代信息论的奠基人香农提出的为科学界公认的理论，在一个存在噪声的信道里，可以可靠地传输的最大速率是

$$C = W \log_2 (1 + P/N)$$

其中：

C 是信道内可以可靠传输的最高码率（以比特/秒为单位），称之为信道容量；
W 是信道带宽（以赫兹或 1/秒为单位）；
P/N 是信道的信噪比（即信号功率与噪声功率之比）。

按照这一理论，要想在一个带宽确定而存在噪声的信道里可靠地传送信号，无非有两种途径：加大信噪比或在信号编码中加入附加的纠错码。用生活中的例子类比，就好像在一个嘈杂的啤酒馆里要让侍者听到你的要求，你就得提高嗓门（信噪比），反复吆喝（附加的冗余信号）。多年来人们都在试图接近香农提出的码率极限，然而在这两位法国老兄以前，最好的结果所消耗的功率和香农定理比较还有 3.5 分贝的差距。就是说比按照香农定律计算得到的所需功率数值高一倍多。

香农曾经指出，要提高信号编码效率达到信道容量，就要使编码的分段（所谓“编码词”的长度）尽可能加长而且使信息的编码尽可能随机。但是，这带来的困难是计算机科学里经常碰到的“计算复杂性”问题。为了使编码接近香农理论，也许需要使编码词长度为 1000 比特。相应的计算量为 2^{1000}，即约为 10^{301}。为了理解这个数字有多大，只需要指出人类目前所能探索到的宇宙范围里所有原子的总数也只有 10^{80}而已。因此在过去的几十年里尽管各种复杂的编码方案不断涌现，3.5 分贝的距离好像被无比高耸的计算复杂性之墙阻挡而变得不可逾越。

多年来，编码成为数学家的禁脔。编码专家提出种种方案，试图在可接受的计算复杂性条件下设计编码和算法，以提高效率。但我们的这两位法国老兄的数学功底也许并不怎么样，他们没有试图从数学上找突破口，因此他们的论文在会上被怀疑甚至忽略就不足为奇了。在这些专家看来他们根本不是“圈内”的人。用北京土话说就是“棒槌”。

凭着电机工程师的经验，他们发现在电子学中经常用到的反馈概念似乎被数学家们忽略了。也许反馈能够使我们绕过计算复杂性问题。于是他们就设计了一套新的办法。

首先他们摈弃了“纯粹”的数字化概念。在典型的数字化方法中，总是先把某一电平设定为阈值。信号电平高于这一阈值就判决为“1”，低于就判决为“0”。在 Turbo 码解码过程中，某一特定比特的电平被量化为整数，例如从-127 到+127。其数值就作为判决该比特为“1”或“0”的可置信度的度量（例如-110 意味该比特非常非常可能是“0”，而+40 意味该比特也许是“1”但把握不大）。其次，与其他系统不同，Turbo 码系统在发射端和接收端分别设置两个编码器和解码器。其中一对编解码器对特定的一段比特流进行奇偶校验码的加入和校验计算，另一对编解码器则在同一段码流经过交织扰动后对其进行上述同样操作。由于这两段码流包含同样的数据，如果没有信道噪声，解码结果应该一致。但在噪声干扰下两组结果会产生差别。通过上述对比特判决的可置信度信息的帮助，把这两组结果彼此参照，可以得出第一次近似的结果。把这一结果“反馈”到解码器前端，再进行迭代，经过几次迭代两个解码器的结果就会互相接近（收敛）。这样就绕过了计算复杂性问题。当然这样做也得付出代价。由于迭代解码，必然会产生时延。所以对于实时性要求很高的场合，Turbo 码直接应用会受到限制。

使那些编码专家“跌破眼镜”的是，其他小组对这两位法国老兄论文重复检验的结果验证了他们方案的正确性。现在人们谈论的已经是和香农极限相差 0.1 分贝还是 0.01 分贝。这就解决了在信道信噪比很差条件下获得高效率数字通信的难题。因此这一方案受到了从从事深空探测到开发第三代移动通信的各方面工程界人士的重视，很有可能阁下的下一个手机里就会装有一个 Turbo 码模块，让我们拭目以待吧。（编译自《IEEESpectrum》2004 年 3 月号）

（转载自《计算机教育》2004 年第 7 期，本刊增加了原文全文中英文对照）

编译者按：在技术发展史上许多突破性进展是出自名不见经传的“小人物”。他们不顾当时科学权威认定的种种“极限”（甚至也许就不知道这些极限）另辟蹊径，从而突破了理论壁垒。克劳德.伯劳和阿雷恩.格莱维欧克斯发明 Turbo 码就是新的典型案例。如果他们也像当时许多具有坚实数学基础的编码专家那样，从计算复杂性入手，恐怕永远也走不出迷宫。不能由此得出理论无用的结论，因为他们的工作是基于香农的理论；也不能以为侥幸可以代替艰苦的探索，他们的工作是长期工程实践的结晶。然而，Turbo 码的产生过程使我们对创新有了更为深刻地了解。如果我们从事的研究都必须是当时科学家认可的项目，类似 Turbo 码这样的创新就不可能产生。如果一切研究都要经过审批才能立项，那创新就死定了。什么都靠计划、规划许多伟大的科学家和发明家就不可能产生，因为科技史上的革命性突破很多是事先没有规划或计划到的。不是说规划和计划不重要，问题是规划、计划什么，是环境政策为主还是项目为主。这实在值得为政者三思。

附：《Closing in on the perfect code》中英文对照

Closing in on the perfect code

Turbo codes, which let engineers pump far more error-free data through a channel, will be the key to the next generation of multimedia cellphones

By Erico Guizzo

It's not often in the rarefied world of technological

接近完美的编码

Turbo 码使工程师可以在一个信道里传输多得多的无误码数据，从而将成为下一代多媒体移动通信的关键

在超尘脱俗的技术研究领域，

research that an esoteric paper is greeted with scoffing. It's even rarer that the paper proves in the end to be truly revolutionary.

一篇深奥的论文通常很少受到嘲笑。更为罕见的是这篇论文后来竟又被证明是革命性的。

It happened a decade ago at the 1993 IEEE International Conference on Communications in Geneva, Switzerland. Two French electrical engineers, Claude Berrou and Alain Glavieux, made a flabbergasting claim: they had invented a digital coding scheme that could provide virtually error-free communications at data rates and transmitting-power efficiencies well beyond what most experts thought possible.

而这恰恰发生在十年以前，1993 年在瑞士日内瓦举行的 IEEE 国际通信学会。会上两位法国电机工程师克劳德.伯劳和阿雷恩.格莱维欧克斯声称他们发明了一种数字编解码方案，可以实现事实上无误码而码率与发射功率效率超出所有专家预期的传输。

Turbo 码的发明人克劳德.伯劳（左）和阿雷恩.格莱维欧克斯，这两位法国人都是位于布莱斯特的布列塔尼国立高等电信学校的教授。他们解决了困扰通信界近 40 年的一个难题。

FRENCH CONNECTION: Turbo codes inventors Claude Berrou [left] and Alain Glavieux, both professors at the Ecole Nationale Supérieure des Télécommunications de Bretagne in Brest, France, solved a communications puzzle that had lasted for more than 40 years.

The scheme, the authors claimed, could double data throughput for a given transmitting power or, alternatively, achieve a specified communications data rate with half the transmitting energy—a tremendous gain that would be worth a fortune to communications companies.

文章作者宣称，这一方案可以在给定功率下把传输码率提高一倍，或者在给定传输速率下把信号能量减少一半 — 这一进展足以使某些通信公司动心来碰一下运气。

Few veteran communications engineers believed the results. The Frenchmen, both professors in the electronics department at the Ecole Nationale Supérieure des Télécommunications de Bretagne in Brest, France, were then unknown in the information-theory community. They must have gone astray in their calculations, some

几乎没有专家相信他们的结果。这两位法国人都是位于布莱斯特的布列塔尼国立高等电信学校的教授，当时在信息理论领域都是名不见经传的。一些人想当然地认为他们的计算一定有什么错误。结论看来如此不合常理以

reasoned. The claims were so preposterous that many experts didn't even bother to read the paper.

致一些专家懒得去阅读这篇文章。

Unbelievable as it seemed, it soon proved true, as other researchers began to replicate the results. Coding experts then realized the significance of that work. Berrou and Glavieux were right, and their error-correction coding scheme, which has since been dubbed turbo codes, has revolutionized error-correction coding. Chances are fairly good that the next cellphone you buy will have them built in.

似乎不可思议的是，当其他研究人员开始试验重复其结果时，很快证明这些结论是正确的。于是编解码理论专家认识到这篇文章的重要。伯劳和格莱维欧克斯提出的纠错编码方案是对的，这一方案就被命名为 Turbo 编码，它对纠错编码产生了革命性的影响。你买的下一代移动电话很可能就是基于这一编码方案。

From a niche technology first applied mainly in satellite links and in at least one deep-space communications system, turbo codes are about to go mainstream. As they are incorporated into the next-generation mobile telephone system, millions of people will soon have them literally in their hands. This coding scheme will let cellphones and other portable devices handle multimedia data such as video and graphics-rich imagery over the noisy channels typical of cellular communications. And researchers are studying the use of turbo codes for digital audio and video broadcasting, as well as for increasing data speeds in enhanced versions of Wi-Fi networks.

一开始，Turbo 码只是应用于一些特殊场合，主要是用于卫星链路。至少还有一次用于深度空间通信，现在这个技术要走上主流舞台了。当这个技术与下一代移动电话结合，成百万人就会用上它。这一技术会使手机或其它移动设备有能力进行多媒体数据，如视频信号及图形图像信号的通信。由于在这种环境下通常信道噪声严重，其它技术很难满足要求。不仅如此，研究人员还在研究把 Turbo 码用于数字音频和视频广播，以及用于增强型无线互联网，以提高数据传输速率。

With possibilities like these, turbo codes have jumped to the forefront of communications research, with hundreds of groups working on them in companies and universities all over the world. The list includes telecommunications giants like France Télécom and NTT DoCoMo; high-tech heavyweights like Sony, NEC, Lucent, Samsung, Ericsson, Nokia, Motorola, and Qualcomm; hardware and chip manufacturers like Broadcom, Conexant, Comtech AHA, and STMicroelectronics; and start-ups like Turboconcept and iCoding.

由于 Turbo 码的这种巨大前景，它已经成为通信研究的前沿。在全世界各大公司和大学的成百个小组都聚焦在这个领域。其中有电信钜子如法国电信、NTT(日本电话电报公司)、DoCoMo；有高技术公司巨头如索尼、NEC(日本电气)、朗讯、三星、爱立信、诺基亚、摩托罗拉和高通(Qualcomm)；有硬件和芯片制造商如 Broadcom、Conexant、Comtech AHA 和 STMicroelectronics；还有新兴高技术企业如 Turboconcept 和 iCoding

Turbo codes do a simple but incredible thing: they let engineers design systems that come extremely close to the so-called channel capacity—the absolute maximum capacity, in bits per second, of a communications channel for a given power level at the transmitter. This threshold for reliable communications was discovered by the famed Claude Shannon, the brilliant electrical engineer and mathematician who worked at Bell Telephone Laboratories in Murray Hill, N.J., and is renowned as the

Turbo 码其实只是实现了一件简单但了不起的事情 — 使工程师能够设计出非常接近信道容量（即在一定发射功率电平下信道可传输的每秒比特数值的绝对最大容量）的系统。

这一极限值是由当时在贝尔实验室工作的著名的电机工程师和数学家，以信息论之父闻名于世

father of information theory [see sidebar, "Shannon: Cracking the Channel"].

的克劳德.香农发现的。

In a landmark 1948 paper, Shannon, who died in 2001, showed that with the right error-correction codes, data could be transmitted at speeds up to the channel capacity, virtually free from errors, and with surprisingly low transmitting power. Before Shannon's work, engineers thought that to reduce communications errors, it was necessary to increase transmission power or to send the same message repeatedly—much as when, in a crowded pub, you have to shout for a beer several times.

在 1948 年的一篇标志性论文中，香农（2001 年去世）证明在使用正确的纠错码的条件下，数据可以以接近信道容量的速率几乎无误码地传输，而所需的功率却十分低。在香农这篇文章以前，工程师们认为要减少误码，要么就得增加发射功率，要么就得反复发送同一段消息—就好像在人声嘈杂的啤酒馆里人们得大声地反复呼叫要啤酒一样。

Shannon basically showed it wasn't necessary to waste so much energy and time if you had the right coding schemes. After his discovery, the field of coding theory thrived, and researchers developed fairly good codes. But still, before turbo codes, even the best codes usually required more than twice the transmitting power that Shannon's law said was necessary to reach a certain level of reliability—a huge waste of energy. The gap between the practical and the ideal, measured in decibels—a ratio between the signal level and the noise level on a logarithmic scale—was about 3.5 dB. To chip away at it, engineers needed more elaborate codes.

香农从根本上证明了如果你有正确的编码方案就没有必要浪费那么多能量和时间。在他的发现之后编码理论就发展起来了，研究人员找到了相当好的编码方式。但是在 Turbo 码以前，即使最好的编码方案通常也需要香农定理要求的功率的两倍才能达到必要的可靠性—这是能量的巨大浪费。在理论数值和实际要求数值之间的能量差距用对数坐标表示大约为 3.5 分贝。要想缩小这一差距工程师需要更精细的编码。

That was the goal that persisted for more than four decades, until Berrou and Glavieux made their discovery in the early 1990s. When they introduced turbo codes in 1993, they showed it was possible to get within an astonishing 0.5 dB of the Shannon limit, for a bit-error rate of one in
100 000. Today, turbo codes are still chipping away at even that small gap.

这成了近四十年工程界不断努力的目标，一直到伯劳和格莱维欧克斯在九十年代初做出了他们的发现为止。1993 年他们提出 Turbo 码概念时展示了在误码率为十万分之一的情形下把实际功率和香农理论的差距惊人地缩小为 0.5 分贝的可能。今天 Turbo 码甚至还在继续缩小这一已经很小的差距。

The solution to overcoming the noise that plagued all communications channels, according to Shannon's seminal paper, was to divide the data into strings of bits and add to each string a set of extra bits—called parity bits—that would help identify and correct errors at the receiving end. The resulting group of bits—the data bits plus the parity bits—is called a codeword, and typically it represents a block of characters, a few image pixels, a sample of voice, or some other piece of data.

按照香农奠基性的文章，克服困扰所有通信信道的噪声的办法是把要传输的数据划分成一段一段的比特串，在每一段加上额外的比特，称之为奇偶比特，这些码在接收端可以帮助识别和纠正误码。数据比特加奇偶比特所形成的一组比特群称之为编码词，通常表示一段字符、若干像素、一段声音取样或其他数据块。

Shannon showed that with the right collection of codewords—with the right code, in other words—it was possible to attain the channel capacity. But then, which code could do it? "Shannon left unanswered the question of inventing codes," says David Forney, a professor of electrical engineering at the Cambridge-based Massachusetts Institute of Technology (MIT) and an IEEE Fellow. Shannon proved mathematically that coding was the means to reach capacity, but he didn't show exactly how to construct these capacity-approaching codes. His work, nevertheless, contained valuable clues.

IEEE 的会士，麻省理工学院的电机系教授戴维.佛内指出：香农证明了对于一个正确的编码词集合—也就是说正确的编码，有可能达到信道容量。但是，什么编码可以实现这一点？香农没有回答。香农从数学上证明了编码是达到信道容量的手段，但他没有给出如何构建这样的编码的准确方法。但香农的工作提供了宝贵的启示。

Shannon thought of codewords as points in space. For example, the codeword 011 can be considered a point in a three-dimensional space with coordinates $x = 0$, $y = 1$, and $z = 1$. Codewords with more than three bits are points in hyperspace. Noise can alter a codeword's bits, and therefore its coordinates, displacing the point in space. If two points are close to each other and one is affected by noise, this point might fall exactly onto the other, resulting in decoding error. Therefore, the larger the differences in codewords—the farther apart they are—the more difficult it is for noise to cause errors.

香农把编码词当作（编码）空间中的一个点。例如编码词 011 可以当成三维空间中坐标为 x=0,y=1,z=1 的一个点。多于三个比特的编码词可以看成多维空间的点。噪声会扰动一个编码词的比特，从而扰动其在空间的坐标，使其位置发生变化。如果两个点位置靠近，其中一点被噪声影响，这点就有可能正好落到另一点上，形成解码错误。因此，编码词之间的空间距离分得越开，噪声就越难以造成误码。

To achieve capacity, Shannon demonstrated that you should randomly choose infinitely long codewords. In other words, going back to his spatial analogy, if you could make the codewords both random and as long as you wanted, you could put the points arbitrarily far from each other in space. There would be essentially no possibility of one point erroneously falling on another. Unfortunately, such long, random codes are not practical: first, because there is an astronomical number of codewords; second, because this code would be extremely slow to use as you transmitted many, many bits for just one codeword. Still, the random nature of a good code would turn out to be critical for turbo codes.

为了达到信道容量的传输极限，香农证明应该随机地选取无限长度的编码词。如果回到他提出的空间比拟，如果你能够按照你的意愿使编码词尽可能随机、尽可能长，你就能把这些编码词在空间分布得尽可能彼此远离，自然一点错误地落到另一点上的情况就难以发生。可惜这种随机、冗长的编码是不现实的。首先编码词的数量会是天文数字，其次这样做就要发射许多许多比特来表示一个编码词，这种编码使用起来会非常慢。然而编码的随机性对 Turbo 码仍旧是关键。

Coding experts put aside Shannon's ideal random codes, as they concentrated on developing practical codes that could be implemented in real systems. They soon began to develop good codes by cleverly choosing parity bits that constrained codewords to certain values, making these codewords unlikely to be confused with other ones.

编码专家在开发现实世界可以使用的编码时只能把香农的理想随机码放在一边。他们很快就开始利用巧妙地选择奇偶比特，把编码词限制在一定值域来开发有效编码，使编码词彼此之间不易混淆。

For example, suppose we have an eight-bit codeword (seven data bits plus one parity bit). Suppose we further insist that all the codewords have an even number of 1s, making that extra parity bit a 1 if necessary to fulfill that requirement. Now, if any of the eight bits is altered by noise, including the parity bit itself, the receiver knows there was an error, because the parity count won't check—there would be an odd number of 1s.

例如我们有一个 8 比特的编码词（7 位有效比特加一位奇偶比特）。假设我们保持每个编码词“1”的个数是偶数，并通过改变外加的奇偶比特来满足这个要求。现在如果任何一个比特，包括奇偶比特在内被噪声所干扰而发生改变，则接收端就会检测出误码，因为奇偶数不对，“1”的个数变成了奇数。

This basic scheme can detect an error, but it can't correct it—you don't know which bit was flipped. To correct errors, you need more parity bits. Coding experts have come up with numerous and ever more sophisticated ways of generating parity bits. Block codes, Hamming codes, Reed-Solomon codes, and convolutional codes are widely used and achieve very low error rates.

这一方案可以检测出误码却不能纠错—我们无法知道是哪一个比特被改变了。为了纠错需要更多奇偶比特。编码专家提出了许多越来越复杂的产生奇偶比特的方法。区块码(block codes)、海明码(Hamming)、李德所罗门码(Reed-Solomon)和卷积码(convolutional)是几种广泛使用的编码方案，其误码率都很低。

Nevertheless, a computational-complexity problem hounded coding specialists and plagued all these codes. The complexity problem emerges as you figure the cost of a code in terms of the amount of computation required to decode your data. The closer you get to Shannon's limit, the more complicated this process becomes, because you need more parity bits and the codewords get longer and longer.

然而，在这些编码方案中计算复杂性问题困扰着编码专家。当人们估算对所收到的数据进行解码所需要的计算量及由此产生的成本时，计算复杂性问题就浮现出来。越接近香农极限编解码过程就越复杂，因为需要更多的奇偶校验比特因而编码词变得越来越长。

For codewords with just 3 bits, for instance, you have a total of only 2^3, or 8, codewords. To approach capacity, however, you might need codewords with, say, 1000 bits, and therefore your decoder would need to search through an unimaginably large collection of 2^{1000}—approximately 10^{301}—codewords. For comparison, the estimated number of atoms in the visible universe is about 10^{80}.

例如，对于长度为 3 个比特的编码词，所有不同词汇总量仅为 2^3，即 8 个。要逼近信道传输极限，就可能需要长度为 1000 比特的编码词，解码器就得遍寻一个大得无法想象的集合—2^{1000}大约10^{301}个编码词汇。而人类所能探索到的宇宙的原子总数也才是10^{80}而已。

The upshot was that if you set about exploiting the best existing codes as your strategy for achieving arbitrarily reliable communications at Shannon's limit, you would be doomed to failure. "The computational complexity is just astronomical," says IEEE Fellow R. Michael Tanner, a professor of electrical and computer engineering and provost at the University of Illinois at Chicago. "These codes don't have the capability to do it." How could researchers get past this barrier? It was hopeless, some actually concluded in the late 1970s.

结论只能是如果要设法用已有编码方案，即使是最好的，来达到香农极限下的可靠通信注定是不可能的。按照伊利诺伊大学电机系教授塔纳的说法，现有编码不可能达到香农极限，因为计算复杂性达到天文数字程度。看不到克服这一壁垒的途径。七十年代末，不少人认为没有希望解决这一问题。

Turbo codes solved the complexity problem by splitting it into more manageable components. Instead of a single encoder at the transmitter and a single decoder at the receiver, turbo codes use two encoders at one end and two decoders at the other [see illustration, "How Turbo Codes Work"].

通过把编码分成若干易于处理的“组件”Turbo 码解决了计算复杂性问题。和现有多数系统在发射端只有单个编码器，接收端只有单个解码器不同，Turbo 码在一端用两个编码器另一端用两个解码器。

Researchers had realized in the late 1960s that passing data through two encoders in series could improve the error-resistance capability of a transmission—for such a combination of encoders, the whole is more than the sum of the parts. Turbo codes employ two encoders working synergistically—not in series, but in parallel.

研究人员在 60 年代末发现传输数据通过两个串接的编码器可以使传输数据具有更强的抗误码能力—在这种情形下整体大于各部分之和。Turbo 码则利用两个联合工作的编码器，不是串接而是并接。

The turbo process starts with three copies of the data block to be transmitted. The first copy goes into one of the encoders, where a convolutional code takes the data bits and computes parity bits from them. The second copy goes to the second encoder, which contains an identical convolutional code. This second encoder gets not the original string of bits but rather a string with the bits in another order, scrambled by a system called an interleaver. This encoder then reads these scrambled data bits and computes parity bits from them. Finally, the transmitter takes the third copy of the original data and sends it, along with the two strings of parity bits, over the channel.

Turbo 编码过程一开始就把要传输的数据块制成三份拷贝。第一份拷贝送到两个编码器之一然后通过卷积编码器从数据比特计算出奇偶校验比特。第二份拷贝送到第二个编码器，里面也有一份完全一样的卷积编码器。第二个编码器得到的比特流次序和原来不同，是经过一个交织器系统加扰的。然后由这个编码器读出经过扰动的比特流并从中计算出奇偶校验比特。最后发射器把原来数据的第三份拷贝和上面两组奇偶校验码一起沿着信道发送出去。

That rearranging of the bits in the interleaver is the key step in the whole process. Basically, this permutation brings more diversity to the codewords; in the spatial analogy, it pushes the points farther apart in space. "The role of the permutation is to introduce some random behavior in the code," says Berrou. In other words, the interleaver adds a random character to the transmitted information, much as Shannon's random codes would do.

整个过程的关键是交织器对比特顺序的重组。这一重新排列增加了编码词的参差性；用空间概念理解相当在比特空间把编码词之间的距离拉开了。按照伯劳的说法，重新排列的作用是在编码中引入某种随机行为。换句话说，交织器在发射的信息中加入了随机特征，作用类似香农的随机码。

But then turbo codes, like any other code with a huge number of codewords, would also hit the wall of computational complexity. In fact, turbo codes usually work with codewords having around a thousand bits, a fairly unwieldy number. Hopeless? Yes, if you had a single decoder at the receiver. But turbo codes use two component decoders that work together to bypass the

但像其他编码词汇量很大的编码系统一样，Turbo 码也会碰到计算复杂性之墙。其实 Turbo 码通常是用大约 1000 比特编码词工作，非常不利的长度。没有希望了吗？如果在接受端只有一个编码器，确实如此。可是 Turbo 码用两个分量解码器绕过了复杂性问题。

complexity problem.

The role of each decoder is to get the data, which might have been corrupted by noise along the channel, and decide which is the more likely value, 0 or 1, for each individual bit. In a sense, deciding about the value of each bit is as if you had to guess whether it's raining or not outside. Suppose you can't look out a window and you don't hear any sounds; in this case, you basically have no clue, and you can simply flip a coin and make your guess. But what if you check the forecast and it calls for rain? Also, what if you suddenly hear thunder? These events affect your guess. Now you can do better than merely flipping a coin; you'll probably say there's a good chance that it is raining and you will take your umbrella with you.

每个解码器的作用都是获取数据，在信道噪声影响下，数据可能被破坏，所以两个解码器还要判断所收到的每一比特数据究竟更可能是“1”还是“0”。这有点像在屋子里猜外面否在下雨，而你又无法从窗户里看到外面，也听不到外面的声音。这种情况下你没有任何“迹象”作依据，也许只能靠抛硬币看那面冲上来进行猜测。可是如果你能看到天气预报，而且天气预报说要下雨，情形又如何呢？还有，要是你突然听到雷声又如何呢？这些事件都会影响你的猜测。这时情形可以比抛硬币有所改进。你也许会说正在下雨的机会大一些，而且你可能带把伞出门。

Each turbo decoder also counts on "clues" that help it guess whether a received bit is a 0 or a 1. First, it inspects the analog signal level of the received bits. While many decoding schemes transform the received signal into either a 0 or a 1—therefore throwing away valuable information, because the analog signal has fluctuations that can tell us more about each bit—a turbo decoder transforms the signal into integers that measure how confident we can be that a bit is a 0 or a 1. In addition, the decoder looks at its parity bits, which tell it whether the received data seems intact or has errors.

每个 turbo 解码器也考虑“迹象”来帮助其猜测收到的比特是“0”还是“1”。首先，检验收到的比特的信号电平。许多解码方案把收到的信号直接转换成“0”或“1”，因此把非常有价值的信息抛弃了。模拟信号会产生涨落起伏，这会给我们关于每一比特的更多信息。Turbo 解码把信号转换成整数，用其可以度量信号是“0”还是“1”的可信度。此外解码器还观察奇偶校验码，从中可以得知所收到的比特是否有误码。

The result of this analysis is essentially an informed guess for each bit. "What turbo codes do internally is to come up with bit decisions along with reliabilities that the bit decisions are correct," says David Garrett, a researcher in the wireless research laboratory at Bell Labs, part of Lucent Technologies, Murray Hill, N.J. These bit reliabilities are expressed as numbers, called log-likelihood ratios, that can vary, for instance, between -7 and +7. A ratio of +7 means the decoder is almost completely sure the bit is a 1; a -5 means the decoder thinks the bit is a 0 but is not totally convinced. (Real systems usually have larger intervals, like -127 to +127.)

这些分析的结果对于“猜测”每一比特非常有用。按照贝尔实验室的戴维.伽瑞特的话：Turbo 码从内部看就是在比特判决过程中利用判据可靠性信息。这种比特可靠性用数字表示，称之为对数似然性系数，其取值范围例如可以在-7 到+7 之间。+7 意味解码器几乎可以肯定该比特是“1”；而-5 意味解码器判断该比特是“0”但不是完全有把握。（实际系统常常采用更大的间距，例如从-127 到+127）

Even though the signal level and parity checks are helpful clues, they are not enough. A single decoder still can't always make correct decisions on the transmitted bits and often will come up with a wrong string of bits—the

尽管信号电平和奇偶校验是非常有用的“迹象”但对做出判决仍嫌不够。单一的解码器还不能保证判决总是正确，常常产生错误的码流。解码器会在编码词空间迷失，作为其数据解码结果所

decoder is lost in a universe of codewords, and the codeword it chooses as the decoded data is not always the right one. That's why a decoder alone can't do the job.

选择的编码词未必总是正确的。所以单一解码器不能完成任务。

But it turns out that the reliability information of one decoder is useful to the other and vice versa, because the two strings of parity bits refer to the very same data; it's just that the bits are arranged in a different order. So the two decoders are trying to solve the same problem but looking at it from different perspectives.

但一个解码器的判决可靠性信息对另一解码器也是有用的，因为两个码流的奇偶校验比特实际上是对同一组数据得出的；只不过比特顺序排列作了改变。因此两个解码器实际上是在解同一问题，但观察的视图不同。

The two decoders, then, can exchange reliability information in an iterative way to improve their own decoding. All they have to do, before swapping reliability strings, is arrange the strings' content in the order each decoder needs. So a bit that was strongly detected as a 1 in one decoder, for example, influences the other decoder's opinion on the corresponding bit.

这样，两个解码器就可以用迭代的方式交换可靠性信息来改进各自的解码结果。要求就是把码流内容按照每个解码器工作的需要重新排列顺序，然后在两个解码器之间交换可靠性码流。使得一个解码器对某一特定比特做出的判决，例如强烈认为该比特为“1”，这一信息能够对另一解码器对相应比特的判决产生影响。

In the rain analogy, imagine you see a colleague going outside carrying an umbrella. It's a valuable additional piece of information that would affect your guess. In the case of the turbo decoders, now each decoder not only has its own "opinion," it also has an "external opinion" to help it come up with a decision about each bit. "It's as if a genie had given you that information," says Gerhard Kramer, a researcher in the mathematical sciences research center at Bell Labs. This genie whispers in your ear how confident you should be about a bit's being a 1 or a 0, he says, and that helps you decode that bit.

就像在猜测是否下雨的那个比喻一样，假如你看到你的同事拿着伞出去了，这对于影响你的猜测应该是非常有用的信息。在 Turbo 解码器的例子中，每个解码器不仅有其自己的“观点”，还得到了外界观点的帮助来对每一比特做出判决。贝尔实验室数学研究中心的杰哈德.卡拉米说，就好像有一个精灵在给你信息，精灵在你耳边悄悄告诉你每个比特为“1”或“0”的可信度有多大，这将帮助你做出判决。

At the heart of turbo coding is this iterative process, in which each component decoder takes advantage of the work of the other at a previous decoding step. After a certain number of iterations, typically four to 10, both decoders begin to agree on all bits. That means the decoders are not lost anymore in a universe of codewords; they have overcome the complexity barrier.

Turbo 编解码的核心是这一迭代过程，其中每一解码器利用了另一解码器在上一步解码过程得到的结果。在若干次迭代（通常为 4 到 10 次）之后，两个解码器就在所有的比特的判定上一致了。这就意味解码器不会在编码词空间迷失，从而克服了复杂性壁垒。

"It's a divide-and-conquer solution," says Robert J. McEliece, a professor of electrical engineering at the California Institute of Technology, in Pasadena, and an IEEE Fellow. "It broke the problem into two smaller pieces, solved the pieces, and then put the pieces back

加州理工大学的罗伯特.麦克艾立斯教授说“这是个分而治之的解决方案，把问题分解成两个小一些的问题，然后再把结果拼起来”。

together."

伯劳斯指出：也可以从猜纵横字谜的角度来理解 Turbo 解码过程。假想 A 解决了一个纵横字谜，要传送给 B。在一个无噪声信道，只要传送词汇阵列就够了。但在一个噪声信道，阵列中的字母会被搞乱。当 B 收到字谜答案时，许多词无法辨认。为了帮助 B 纠错，A 可以把水平词汇和竖直词汇的“迹象”也传给 B。这是多余的信息，因为字谜已经解开了，但这确实 对 B 有帮助。因为和奇偶校验比特一样，这一信息对可以放进阵列的词汇加了约束。这是一个二维问题，行的解有助于得到列的解，反之亦然，就好像在 Turbo 解码中两个解码器互相帮助一样。

Another way of thinking about the turbo decoding process is in terms of crossword puzzles, Berrou says. Imagine that Alice solved a crossword and wanted to send the solution to Bob. Over a noiseless channel, it would be enough to send the array with the words. But over a noisy channel, the letters in the array are messed up by noise. When Bob receives the crossword, many words don't make sense. To help Bob correct the errors, Alice can send him the clues for the horizontal and vertical words. This is redundant information, since the crossword is already solved, but it nevertheless helps Bob, because, as with parity bits, it imposes constraints on the words that can be put into the array. It's a problem with two dimensions: solving the rows helps to solve the columns and vice versa, like one decoder helping the other in the turbo-decoding scheme.

回顾 11 年前，当 42 岁的伯劳穿过日内瓦会展中心的走廊时，从人们的肩膀上望过去看到许多出席者试图弄懂他们的论文。在演讲过程中年轻的博士生和老练的编解码专家挤满了演讲厅，有些人挤在门边。当伯劳和格莱维欧克斯结束演讲时许多人涌上来要求进一步给出解释，或者只是简单地握握手。

Flash back 11 years as an amused 42-year-old Berrou wanders the corridors of the convention center in Geneva, peeking over the shoulders of other attendees and seeing many of them trying to understand his paper. At the presentation, young Ph.D. students and a scattering of coding veterans pack the auditorium, with people standing by the door. When Berrou and Glavieux finish, many surround them to request more explanations or simply to shake their hands.

让怀疑者信服花了不少时间，伯劳回忆说数字通信需要很坚实的数学基础，一般都认为纠错码是数学家的领地。

Still, convincing the skeptics that the work had no giant overlooked error took time. "Because the foundation of digital communications relied on potent mathematical considerations," Berrou recollected later, "error-correcting codes were believed to belong solely to the world of mathematics."

使伯劳和格莱维欧克斯取得突破的不是什么深奥的定理而是要解决现实世界电信问题的探求努力。在 80 年代末当他们开始在编码方案方面工作时他们惊讶地发现在电子学领域广泛应用的反馈原理在数字接收机研究中从来没有得到应用。

What led Berrou and Glavieux to their important breakthrough was not some esoteric theorem but the struggle to solve real-world problems in telecommunications. In the late 1980s, when they began to work on coding schemes, they were surprised that an important concept in electronics—feedback—was not used in digital receivers.

在放大器中，输出信号总有一小部分回馈到输入端，以保持放大器的性能稳定。伯劳和格莱维欧克斯想为什么这一方法在编解

In amplifiers, a sample of the output signal is routinely fed

back to the input to ensure stable performance. Berrou and Glavieux wondered, why shouldn't it work for coding as well?

码中就不能应用？

They ran the first experiments with their novel coding scheme in 1991 using computer simulations, and when the results came out, they were stunned. "Every day I asked myself about the possible errors in the program," says Berrou.

1991 年他们第一次用计算机模拟实验他们的新编解码方案，当结果出来以后他们大吃一惊。伯劳说“ 那时我每天都问自己是不是程序有什么毛病。”

The first thing Berrou and Glavieux did after confirming that their results were correct was to patent the invention in France, Europe, and the United States. At the time, France Télécom was the major sponsor of their work, so the French company took possession of the turbo code patents. The inventors and their institution, however, share part of the licensing profits. (Turbo codes were not patented in Asia, where they can therefore be used for free.)

伯劳和格莱维欧克斯在确认他们的结果无误以后做的第一件事就是为他们的发明申请法国、欧洲和美国专利。当时法国电信是他们研究工作的主要资助者。所以这家法国公司拥有 turbo 编解码的有关专利。但是发明者和他们所在的学校分享部分许可收益。(Turbo 码在亚洲没有申请专利，因此在亚洲可以免费使用。)

It was France Télécom that asked Berrou to come up with a commercial name for the invention. He found the name when one day, watching a car race on TV, he noticed that the newly invented code used the output of the decoders to improve the decoding process, much as a turbocharger uses its exhaust to force air into the engine and boost combustion. Voilà: "turbo codes"!

法国电信要伯劳为这一编码方案起一个商品名字。有一天他在电视里看汽车比赛时想出了现在的这个名字。他注意到新发明的编解码利用解码器的输出来改进解码过程，和涡轮增压(turbocharger)用排出的气体把空气压入引擎提高内燃机效率的原理很类似，于是就起了“ Turbo 码 ”这个名字

Turbo codes are already in use in Japan, where they have been incorporated into the standards for third-generation mobile phone systems, known officially as the Universal Mobile Telecommunications System (UMTS). Turbo codes are used for pictures, video, and mail transmissions, says Hirohito Suda, director of the Radio Signal Processing Laboratory at NTT DoCoMo, in Yokosuka, Japan. For voice transmission, however, convolutional codes are used, because their decoding delays are smaller than those of turbo codes.

在日本 Turbo 码已经得到应用，成为第三代移动通信，其正式名称为“ 通用移动电信系统 ”—UMTS，标准的一部分。Turbo 码被用于图像、视频和邮件传送。但语音仍用卷积码。因为其解码时延小于 turbo 码。

In fact, the decoding delay—the time it takes to decode the data—is a major drawback to turbo codes. The several iterations required by turbo decoding make the delay unacceptable for real-time voice communications and other applications that require instant data processing, like hard disk storage and optical

事实上解码时延（解码过程所用的时间）是 Turbo 码的主要弱点。解码所需的几次迭代使时延在实时语音通信和其他需要即时数据处理的应用场合（如硬盘数据存取和光传输等）变得无法接受。

transmission.

For systems that can tolerate decoding delays, like deep-space communications, turbo codes have become an attractive option. In fact, last September, the European Space Agency, based in Paris, France, launched SMART-1, the first probe to go into space with data transmission powered by turbo codes. ESA will also use the codes on other missions, such as Rosetta, scheduled for launch early this year to rendezvous with a comet. The National Aeronautics and Space Administration, in Washington, D.C., is also planning missions that will depend on turbo codes to boost reliable communications. "The first missions that will be using these codes will be Mars Reconnaissance Orbiter and Messenger," says Fabrizio Pollara, deputy manager of the communications systems and research section at NASA's Jet Propulsion Laboratory in Pasadena, Calif.

对于可以容忍解码时延的应用如深空通信，turbo 码成为极有吸引力的选择。事实上欧洲航天局去年九月发射的 SMART—1，第一个深空探测器，就使用了基于 Turbo 码的数据传输设备。欧空局在其他航天任务中也会选择这种编码，像定于今年发射的与彗星会合的罗塞塔（Rosetta)。美国国家宇航局也计划在未来的任务中用 Turbo 码提升通信的可靠性。第一个使用这种编码的将是火星轨道勘测器。

Beyond error correction, turbo codes are helping Mobile devices achieve better reception

除了纠错，Turbo 码还可以提高移动装置的接收性能

Digital audio broadcasting, which provides CD-quality radio programs, and satellite links, such as the new Global Area Network of Inmarsat Ltd., in London, are both also about to incorporate turbo codes into their systems.

And beyond error correction, turbo codes—or the so-called turbo principle—are also helping engineers solve a number of communications problems. "The turbo-coding idea sparked lots of other ideas," says Lajos Hanzo, a professor in the School of Electronics and Computer Science at the University of Southampton, United Kingdom, and an IEEE Fellow. One example is in trying to mitigate the effects of multipath propagation—that is, signal distortion that occurs when you receive multiple replicas of a signal that bounced off different surfaces. Turbo codes may eventually help portable devices solve this major limitation of mobile telephony.

提供 CD 质量的数字音频广播和卫星链路，像新成立的海事卫星全球网公司,都在计划把 Turbo 码用于他们的系统。

除了纠错，turbo 码，或 turbo 原理也对工程师解决通信中的一系列问题有所裨益。英国南安普敦大学电子与计算机科学系教授拉杰斯.汉索认为 turbo 码激发了许多灵感。一个例子就是消除多径效应——一种由于信号在不同表面被反射到接收机引起的信号失真。Turbo 码可能可以为结决移动电话的这一主要困难提供帮助。

最后，Turbo 码使研究人员认

Finally, another major impact of turbo codes has been to make researchers realize that other capacity-approaching codes existed. In fact, an alternative that has been given a new lease on life is low-density parity check (LDPC) codes, invented in the early 1960s by Robert Gallager at MIT but largely forgotten since then. "In the 1960s and 1970s, there was a very good reason why nobody paid any attention to LDPC codes," says MIT's Forney. "They were clearly far too complicated for the technology of the time."

识到还存在其他实现容量极限的编码方式。实际上最近提出的低密度奇偶校验码（LDPC）就是一个新的方向。这个方法是 60 年代初由麻省理工的罗伯特.盖拉格发明的，很长时间里被人们遗忘了。在 60、70 年代有很多理由使人们忽视这个发明。它对于当时的技术来说是太复杂了。

Like turbo codes, LDPC attains capacity by means of an iterative decoding process, but these codes are considerably different from turbo codes. Now researchers have implemented LDPC codes so that they actually outperform turbo codes and get even closer to the Shannon limit. Indeed, they might prove a serious competitor to turbo codes, especially for next-generation wireless network standards, like IEEE 802.11 and IEEE 802.16. "LDPC codes are using many of the same general ideas [as turbo codes]," says Caltech's McEliece. "But in certain ways, they are even easier to analyze and easier to implement." Another advantage, perhaps the biggest of all, is that the LDPC patents have expired, so companies can use them without having to pay for intellectual-property rights.

类似于 Turbo 码，LDPC 也是通过迭代达到通信容量极限。但这种编码和 Turbo 码明显不同。现在研究人员已经实现了 LDPC，其性能超过了 Turbo 码，而且更接近香农极限。其实研究人员现在可以提供一系列与 Turbo 码竞争的编解码方案，特别是用于下一代移动通信网络标准，如 IEEE802.11 和 IEEE802.16。LDPC 使用了和 Turbo 码同样的基本概念，但这种编码更容易分析、更容易实现。还有一条也许是最最重要的，其专利已经过期，所以公司可以使用而不必付费。

Turbo codes put an end to a search that lasted for more than 40 years. "It's remarkable, because there's this revolution, and nowadays if you can't get close to Shannon capacity, what's wrong with you?" says the University of Illinois's Tanner. "Anybody can get close to the Shannon capacity, but let's talk about how much faster your code goes...and if you are 0.1 dB from Shannon or 0.001 dB."

Turbo 码结束了一场持续了 40 年的探求。这是划时代的，因为这是革命性的进展。今天如果你不能接近香农极限就会问：“出了什么毛病？”任何人都能接近香农极限，但今天我们谈的是你的编码比别的编码快多少以及你离香农极限差 0.1 分贝还是 0.001 分贝。

It was the insight and naiveté typical of outsiders that helped Berrou and Glavieux realize what the coding theory community was missing. "Turbo codes are the result of an empirical, painstaking construction of a global coding/decoding scheme, using existing bricks that had never been put together in this way before," they wrote a few years ago.

是直觉和质朴帮助伯劳和格莱维欧克斯认识到被编码理论界忽视了的东西。几年以前他们写道“Turbo 码是经验、苦干的结果，是从全局考虑构建的编解码方案，所使用的各种技术元素都是已有的，只是以前从未以这种方式整合而已。”

Berrou says their work is proof that it is not always

伯劳指出他们的工作证明并非总是需要知道理论的极限才能达到这些极限。这使人们想起一个

necessary to know about theoretical limits to be able to reach them. "To recall a famous joke, at least in France," he says, "the simpleton didn't know the task was impossible, so he did it."

法国著名的笑话：傻瓜不知道这件事是没法做到的，因此他就做到了。

SHANNON: CRACKING THE CHANNEL

1948 年克劳德.香农发表了他著名的划时代论文《通信的一个数学理论》，当时他还只是贝尔实验室的一个年轻工程师。

在文章里香农对当时还很模糊的“ 信息 ”这个概念下了定义，使其得以量化。按照他的理论，信息的基本单位是比特。

香农证明了对于每一个特定信道，所能可靠传输的数据量有一个最大值，称之为信道容量，用比特每秒度量。他证明只要按照正确的方式编码就可以几乎无误码地达到信道容量。这一结果使当时的工程界大吃一惊。

信道容量成为衡量通信系统的“ 标杆 ”。在很多情形下信道容量可以用以下公式表达：

$C = W \log_2 (1 + P/N).$

其中 C 是信道容量，单位是比特/秒；W 是带宽，以赫兹为单位；P 是发射信号功率；N 为噪声功率，均以瓦为单位。

从空间探测到手机和光盘播放器这些使我们的生活更加舒适和丰富多彩的产品和系统里都蕴含着以香农理论为基础的数字技术。

香农于 2001 年 2 月 24 日逝世，享年 84 岁。

In 1948, Claude Shannon, then a young engineer working at Bell Telephone Laboratories in Murray Hill, N.J., published a landmark paper titled "A Mathematical Theory of Communication."

In that paper, Shannon defined what the once fuzzy concept of "information" meant for communications engineers and proposed a precise way to quantify it: in his theory, the fundamental unit of information is the bit.

Shannon showed that every communications channel has a maximum rate for reliable data transmission, which he called the channel capacity, measured in bits per second. He demonstrated that by using certain coding schemes, you could transmit data up to the channel's full capacity, virtually free of errors—an astonishing result that surprised engineers at the time.

"I can't think of anybody who could ever have guessed that such a theory existed," says Robert Fano, an emeritus professor of computer science at the Massachusetts Institute of Technology, in Cambridge, and a pioneer in the information theory field. "It's just an intellectual jump; it's very profound."

The channel capacity became an essential benchmark for communications engineers, a measure of what a system can and cannot do, expressed in many cases by the famous formula,

$C = W \log_2 (1 + P/N).$

In the formula, C is the capacity in bits per second, W is the bandwidth in hertz, P is the transmitter power in watts, and N is the noise power, also in watts.

From space probes to cellphones and CD players, Shannon's ideas are invisibly embedded in the digital technologies that make our lives more interesting and comfortable.

A tinkerer, juggling enthusiast, and exceptional chess player, Shannon was also famous for riding the halls of Bell Labs on a unicycle. He died on 24 February 2001, at age 84, after a long battle with Alzheimer's disease.

作者: **中国科学院计算技术研究所 顾问、《信息技术快报》主编**