Perfect Shuffles and Their Relation to Math

A magician's trick turns out to be based on a very hard mathematics problem. Three researchers now have solved the problem

Persi Diaconis, a slow-talking statistician from Stanford, takes a deck of cards from his briefcase. He has come to talk about the mathematics of perfect shuffles and, he says, "You can't talk about a perfect shuffle without seeing one." He divides the cards in two piles and then quickly does a riffle shuffle. The two stacks are perfectly interlaced in the shuffled deck.

Diaconis, who ran away from home at age 14 to become a magician, is one of only about 200 of the tens of thousands of magicians in the world who can do a perfect shuffle. And he is one of only about 25 who can do eight perfect shuffles in a row to bring a 52-card deck back in order. His lifelong fascination with these shuffles led him to an intriguing and very difficult mathematics problem—How can you characterize all the possible arrangements of cards when a deck, containing an arbitrarily chosen number of cards, is perfectly shuffled over and over again?

Diaconis, working with Ronald Graham of Bell Laboratories and William Kantor of the University of Oregon, has spent the past 6 months working on and solving this problem. The solution turns out to be related to problems in group theory, one of the most theoretical areas of mathematics, and to problems in computer science, one of the most applied areas of mathematics. The story of how these researchers came upon and solved the perfect shuffle problem is one of coincidences and surprising interconnections in mathematics. And it illustrates, says Kantor, that although "shuffling sounds like a ridiculous thing to be paid to think about, it really isn't. It's not as silly as it sounds."

Perfect shuffles, Diaconis explains, are of two types, called "in" and "out." Both types start out the same. A deck of cards is divided exactly in half and the two halves are shuffled so that they are perfectly interlaced. An "out" shuffle, leaves the original top card of the deck on top of the shuffled deck. In an "in" shuffle, the original top card is the second from the top of the shuffled deck.

"I have done perfect shuffles for years," Diaconis says. "When I was a kid, I noticed something interesting." He found that if he wanted to get the top card of the deck into a particular position, say the fourteenth from the top of the deck, all he had to do was express the number 14 − 1, or 13, in binary notation, as 0's and 1's. Then if he thought of each 0 as an out shuffle and each 1 as an in shuffle and did that sequence of shuffles, the top card showed up where he wanted it—in this case, in position 14.

Diaconis was intrigued. He generalized the problem and asked how one could follow the rearrangements of a deck that occur with sequences of in and out shuffles. "I brooded on and off about this problem for close to 25 years," he says. "It turns out to be a very hard problem."

He looked for clues in books on cheating at cards and found that references to cheating by means of perfect shuffles go back to 1726. But no magicians or card sharks ever solved the mathematical problem that Diaconis posed. Then, last year, Diaconis and other faculty members at Stanford received a letter from Donald Knuth, a computer science professor at Stanford, saying that he had some students in a programming course who, as part of their course work, were to help solve faculty members' computing problems. Diaconis and the other faculty members were asked if they had any good problems for the students.

Diaconis immediately thought of his card-shuffling problem. "I just couldn't touch that problem theoretically," he recalls, so he thought perhaps one of Knuth's students could make some progress on a computer by brute force.

"Persi's problem appealed to Eric Hamilton," says Knuth, explaining that Hamilton, an undergraduate student began by programming the Stanford computer to determine all possible card rearrangements resulting from perfect shuffles of decks of various sizes. But he soon found that he could not go farther than decks of ten cards because the number of possibilities became so large. Even for a deck of ten cards it took the computer 20 minutes to do the calculations.

The next step was to try to be more clever about the computer programming. In group theory, Diaconis remarks, there are some ingenious computer algorithms that mathematicians devised to determine the order of a group with a given set of generators—a problem analogous to the problem of the perfect shuffle. Hamilton and Diaconis decided to use one of these algorithms developed by Charles Sims of Rutgers University. The Sims algorithm, Diaconis says, "is a totally non-obvious way of working with these objects [the generators of groups] on a computer." Knuth, who by this time was also intrigued by Diaconis' problem, made some improvements in Sims' algorithm and they were set to go.

Hamilton programmed the computer to calculate the order of the shuffle group—how many different card combinations can occur—for decks up to size 52. Even with the Sims algorithm, this was a difficult problem, taking 4 hours of computer time.

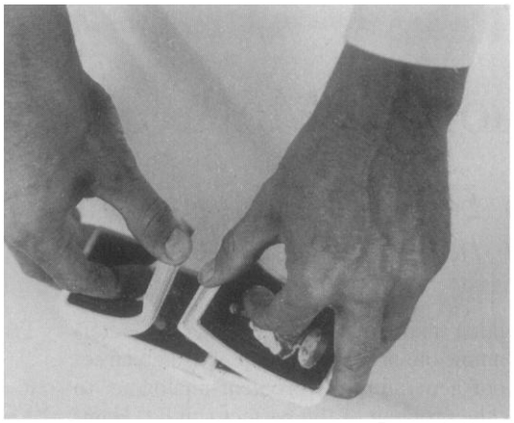
"Now we had these lists of numbers giving us the number of arrangements for each deck size," Diaconis says. "We stared at them and tried to think what on earth is going on. There is a pattern but it doesn't start until after 24 cards. Before 24 cards, the numbers are chaotic. After 24 cards, the pattern repeats every 8 cards."

To explain what kind of pattern they saw, Diaconis notes that magicians have known for quite some time that both in and out shuffles preserve a certain symmetry. The cards are rearranged as sets of pairs, each card of a pair being equally distant from the center of the deck. For example, after an out shuffle the original top and bottom cards of the deck remain on the top and the bottom. After an in shuffle, the original top and bottom cards are second from the top and second from the bottom. Symmetric pairs also can be flipped in place by perfect shuffles.

It looked like every possible pattern of cards occurs subject to the constraint that central symmetry must be preserved. In some cases the number of patterns of cards would be one-half or one-fourth of the total number possible with the symmetry constraint. Thus for 52 cards, he guessed that there would be $2^{26} \times 26!$ possible arrangements. For $2n$ cards there would be $2^n \times n!$ conceivable arrangements, he guessed.

But it is one thing to guess at an answer to a mathematical problem and it

0036-8075/82/0430-0505$01.00/0



Bettman Archives

is another thing to prove that your answer is correct. It took Diaconis and two others 6 months to prove that their guess was correct. Why did they persevere?

One thing that motivated Diaconis was his chance discovery that a great mathematician, Paul Levy, had worked on a variation of the same problem. Shortly after Hamilton had done the computer calculations Diaconis was browsing in the Stanford Library and happened to pick up a book of Levy's collected works. To his surprise, Diaconis noticed that Levy had worked on equations telling how many perfect in shuffles or out shuffles are necessary before particular cards in decks of various sizes come back to their original position. He had carefully calculated by hand the answers for some simple cases but did not solve the equations in general.

"In his book, Levy never mentioned why he was doing his work. He just presented it as a math problem and never tied it to card shuffling," Diaconis says. Diaconis was encouraged, however. "Often you work on math problems and nobody cares about them but you. But Levy's such a smart guy and he got so many important results that I thought there was a good chance that this problem is important," he says.

Diaconis went to Bell Laboratories to work with Graham and Kantor, a visitor at the labs. Graham and Diaconis had previously worked on the card-shuffling problem and Graham had solved it for the special case of decks of cards numbering a power of 2, such as 4, 8, 16, 32, or 64. The shuffle group for these decks, says Graham, "is very small. Actually, all you have to know [for decks of cards numbering a power of 2] is the top and bottom card of the deck. That enables you to know where every other card is. In fact, knowing the top and bottom card tells you more than you need to know to determine where all the other cards are." But, Graham explains, these decks are truly a special case—there are far more possible arrangements for decks of other sizes.

When Diaconis came to Bell Labs with Hamilton's computer printout, Graham scrutinized the numbers of possible arrangements. He was struck by the small number of arrangements for deck size 24—the deck size just before the pattern starts. Graham said, "That number of arrangements is so crazily low that something really funny must be going on." He consulted with Robert Calderbank and Neil Sloane of Bell Labs who looked in a table of groups, computed by Sims, to find what groups had that order. It turned out that the shuffle group for 24 cards is a very famous group, called M12 or the Mathieu group of order 12, that was discovered in 1861. It is one of the first finite simple groups to be discovered that is not a member of an infinite family. "The fact that M12 occurs in a natural way from shuffling cards is just amazing," Diaconis says. "Some gambler could have discovered it. It was constructed by mathematicians but there was no way of explaining it."

Once Graham realized that M12 was "just sitting there," he, Diaconis, and Kantor were motivated to see what else was going on. "That was when we got angry at the problem and decided to really grind it out," Diaconis says. Graham agrees. "That's when we decided the problem was more interesting than we suspected," he recalls.

The next morning, Graham called Kantor and asked him if he could solve the problem for deck sizes that are a multiple of 4. This was the most difficult case and Kantor thought about it for a month as he drove across the country from Bell Labs in New Jersey to his home in Oregon. The way he finally solved the problem was to realize how deck sizes that are a power of 2 differ from those that are not a power of 2 and why deck size 24 is such an anomaly. "I had to find a pattern that did not include powers of 2 and did not include 24," Kantor says.

The proof of the theorem giving all the shuffle groups, however, relies on a computer calculation. The proof proceeds by induction but at the end it is necessary to prove that three different shuffles of 24 cards can generate all (½) 24! possible combinations. The easiest way to show this, Diaconis says, is to use a computer.

So in January of this year Diaconis and Graham went to Xerox Parc in Palo Alto. Lyle Ramshaw of Xerox Parc wrote the computer algorithm and the group stood around the computer waiting to see what would come out. When the answer they wanted appeared, Diaconis recalls, "We let out a big whoop. It meant our theorem was proved."

The connection between card shuffling and groups intrigues John Conway of Cambridge University, who is particularly interested in enormous groups that have no apparent ties to anything concrete. As far as anyone knows they are only creations of the minds of mathematicians. But Conway has a hunch that some of these groups may actually be shuffle groups and he is now trying to base a construction of one of the largest of these, called the Monster group, on card shuffling.

Diaconis soon gave a talk on card shuffling at Massachusetts Institute of Technology. To his surprise, quite a number of electrical engineers came to hear him speak. When he asked why they were interested, he learned that they need to know about the mathematics of card shuffling to interconnect computers in networks for parallel processing. In fact, engineers had independently invented the results of Graham for out shuffles of decks that are powers of 2.

Tom Leighton of MIT explains that computer scientists are well aware of the connection between the design of computer networks for parallel processing and card shuffling—they even call the networks "shuffle exchange graphs." But, for now, computer scientists do not need to know the shuffle groups for decks that are other than a power of 2. Nonetheless, Leighton says, Diaconis' work is of at least theoretical interest to computer scientists.

Through all this work, Diaconis could not stop thinking about what had motivated Levy—why had he worked on equations that are exactly tied in to the card-shuffling problem? Diaconis wrote letters to people who had known Levy, asking if they had any ideas about where those equations came from. Lucien LaCam of the University of California at Berkeley and a former student of Levy told Diaconis that he recalled Levy having written a couple of pages in his autobiography about those equations.

Diaconis got a copy of Levy's autobiography and found the passage LaCam referred to. He learned that Levy worked on the equations because he was fooled by a magician. "In 1901, Levy was at a resort and he was fooled by a card trick," Diaconis says, "Fifty years later he was lying sick in bed and he remembered that card trick. He wrote out those equations to try and figure out why it worked."—GINA KOLATA

Additional Reading

P. Diaconis, R. L. Graham, W. M. Kantor, "The mathematics of perfect shuffles," *Advances in Applied Mathematics*, in press.