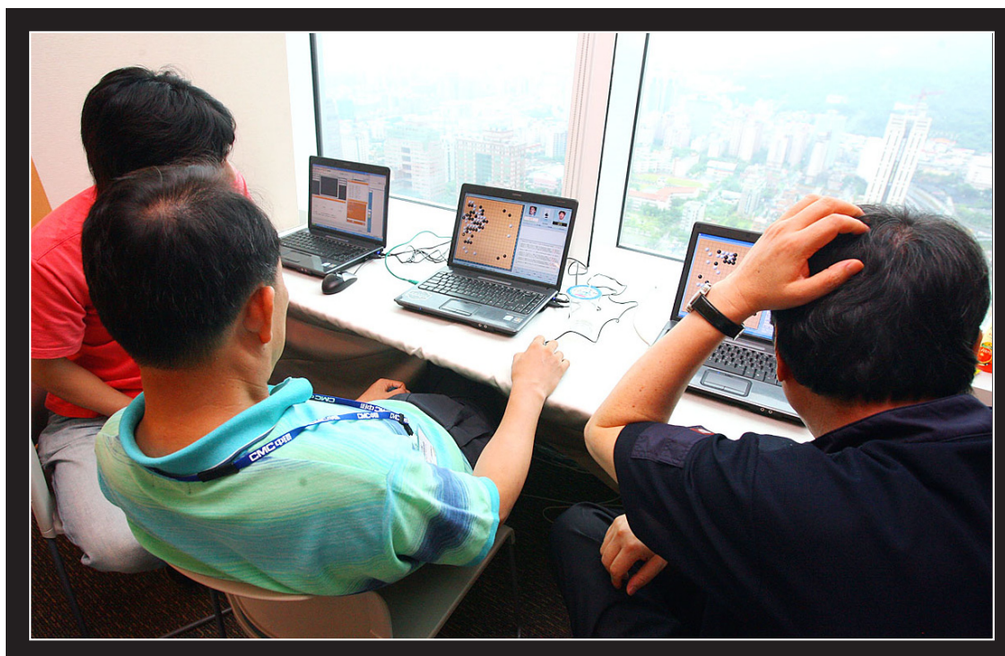

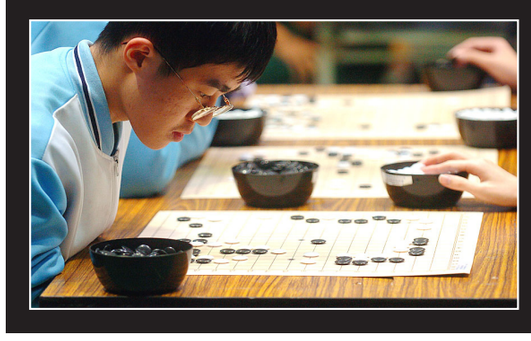

Go, going, gone?

Chess has fallen, draughts has been jumped and now a new algorithm has professionals losing the ancient Chinese game of Go to computers for the first time

BY **ROBERT BLINCOE**
THE GUARDIAN, LONDON

Top left: Teams watch ongoing games on the Internet at the first round of the third CMC Cup World Go Championship in Taipei in 2007.
Middle left: Iyama Yuta, left and Su Yao-kuo face off at the Taiwan-Japan Professional Youth Go Match last June.
Lower left: A player concentrates on his game at the opening day of the Taipei 2007 Student Go Championships.
Top right: Contestants take a break during the Shinkong Masters Cup National Go Open for Children in Taipei in March.
Lower right: Lin Chih-han from Taiwan, left, plays South Korean Park Jungsang in the final at the third CMC Cup World Go Championship.
PHOTOS: TAIPEI TIMES

If you wanted to beat the best software in the world at a classic board game, there was only one left for you — the strategy game Go. It has long been considered the last bastion of human gaming superiority, holding out against the onslaught of computational brute force and artificial intelligence techniques, while draughts, Othello, backgammon and chess have all fallen.

But to be a human winner at Go, you're going to have to get good, very good, in a hurry as the end, with computers ruling, is in sight.

In February, the software MoGo, developed at the University of Paris-Sud, achieved what was once thought impossible: it won two games, on a 19x19 board, against professional Go players. (It did benefit from a handicap — in effect, a number of free turns at the start of the game.) The same month, a program called Many Faces of Go, with a seven-turn handicap, beat a professional in a game played during the general meeting of the Association for the Advancement of Artificial Intelligence. (See the human-computer Go challenges Web page at bit.ly/Go28.)

The wins did require a lot of computing power, however. MoGo was running on 640 cores of the Huygens supercomputer in Amsterdam; Many Faces of Go on a 32-core 3.2GHz Xeon, eight quad cores networked together.

Next month the bar is likely to rise again as programmers fine-tune their code for the annual International Computer Games Association tournament, the computer olympiad, in Pamplona, Spain (bit.ly/Go26).

Yet even a few years ago Go looked like an impossible computing task: the "search space" for each move was too big. At each turn, especially in the beginning, there are hundreds of possible places to play (the board has 361 points, compared to chess's 64), and deciding on which will turn out better a number of moves ahead — a comparatively simple task in chess and draughts — turns into a morass, with hundreds of almost-equal possibilities and a few hundred moves over which to compare them. Standard "minimax" methods that work for chess (picking the move that gives your opponent the fewest high-value moves in future) don't work in Go.

What's changed has been the development of the UCT algorithm (bit.ly/Go24), a special case of the Monte Carlo Tree Search (MCTS) algorithm. UCT first appeared in 2006 applied to small 9x9 Go boards, and now academics, and professional Go programmers, are extending and refining its techniques. It has led to a revolution in Go program development.

David Fotland, the US-based commercial developer behind Many Faces of Go (bit.ly/go222), says the results represent a major leap. But he's realistic about the achievement. "My machine can beat a good amateur, but not a great amateur."

Last year he spent six months incorporating UCT into his software, combined with his traditional Go algorithm ("the new algorithm has some blind spots"), and won that year's computer olympiad. At the event every program incorporating UCT beat all the ones using traditional methods.

Go pieces are called stones, are black or white, and identical. Playing alternately, the object is to use one's stones to surround as many blank intersections (called "territory") as possible. Games typically have a couple of hundred moves.

The Chientan Youth Activity Center in Taipei is filled with children this past January for the 18th Haifong Cup national Go competition. PHOTO: TAIPEI TIMES

The Go rating scale for amateurs starts at 35 kyu, and moves towards 0: the highest level is 1 kyu. The next amateur rank is 1 dan, up to 7 dan. Above them are professionals, who start at pro 1 dan going up to pro 9 dan, the highest level possible.

"Handicapping" allows weaker competitors to play on a level footing with stronger ones: each difference in grading is given as one stone's start. Thus a 20-kyu player would get nine stones in a game against an 11-kyu player.

GAME OF CHANCE

Many Faces of Go's result puts it at about a 1-dan amateur ranking. David Silver, who's researching Go for his PhD at the University of Alberta, says that: "Anyone who would have suggested this [could happen] a couple of years ago would have been laughed out of town."

Silver contributed to MoGo in 2007, developing UCT, which led to the first victories against human pro players on 9x9 boards. But when he started his PhD, pre-UCT, he was discouraged from studying the game by the head of the university's games research group. Too many good minds had been wasted on it, and the research was doomed to failure, it was thought.

For the past 30 years, Go programs have evaluated positions by using handcrafted heuristics based on human knowledge of shapes, patterns and rules. However, professional Go players often play moves according to intuitive feelings that are hard to quantify. Encoding their knowledge into machine-understandable rules has proved to be a dead end.

UCT works on the idea of playing out games over and over again, choosing moves at random, but it is biased to what's been successful before. It does this while still allowing alternative lines to be explored.

Now, Silver says: "I feel very fortunate doing research during this revolutionary period. MCTS is in its infancy, but the rate of performance improvement is pretty rapid." He thinks a machine to beat all humans could appear in four to five years.

Yet humans haven't lost all their tricks. As the human vs computer Go challenges Web page notes: "In every case where each player [computer and human] won at least one game, the human lost the first game played and won the rest. This may be because of experience gained in the first game, or because of techniques learned from discussions with the other players." But the randomization the UCT algorithm brings may make that result less likely.

Fotland thinks the UCT-based work responds to a certain amount of processor supercharging, but then plateaus. "There is a certain kind of large-scale fighting in Go that requires a kind of thinking the algorithm not good at. [The ranking] 1 dan amateur is where people start being good at these large-scale fights."

His rival Mick Reiss, the commercial programmer behind Go++ (bit.ly/AnJ9s), released his version incorporating UCT in Japan this month. His publisher says it matches the Japanese commercial version of Many Faces of Go in strength.

Reiss doesn't think UCT is the total answer. Of pure UCT-based programs, he says: "A lot of them play in a wacky way, which doesn't really work. Because it's so different to what Go players are used to, in the early games they get beaten. Once they get a bit of practice they get their revenge."

The highest level of his own program is based on a combination of the old-style Go approach and the UCT program. "It does less of the strangeness of the pure UCT programs. It plays in a more conventional way."

Fotland is still circumspect about when computers will dominate Go. "I'd say 20 years. There's got to be several algorithm breakthroughs, and 20 years of Moore's law (bit.ly/Go224)."

And then? The end of an era? Certainly. But the end of playing Go? Thankfully, as the evidence shows, we still enjoy the simple pleasure of just playing games.

[TECHNOLOGY]

Why computers are bad at counting votes

Democracy is made difficult by the fact that electronic polling systems are inherently flawed — and open to fraud

BY **WENDY M. GROSSMAN**
THE GUARDIAN, LONDON

It's commonly said that insanity is doing the same thing over and over again while expecting different results. Yet this is what we keep doing with electronic voting machines — find flaws and try again. It should therefore have been no surprise when, at the end of March, California's secretary of state's office of voting system technology assessment decertified older voting systems from Diebold's Premier Election Solutions division. The reason: a security flaw that erased 197 votes in the Humboldt county precinct in last November's presidential election.

Clearly, 197 votes would not have changed the national result. But the loss, which exceeds the error rate allowed under the Help America Vote Act of 2002, was only spotted because a local citizen group, the Humboldt County Election Transparency Project (humtp.com) monitored the vote using a ballot-imaging scanner to create an independent record. How many votes were lost elsewhere?

Humboldt County used Diebold's GEMS operating system version 1.18.19 to tally postal ballots scanned in batches, or "decks." The omission of votes was a result of a flaw in the system, where, given particular circumstances, it deletes the first deck, named "Deck Zero," without noting it in the system's audit logs.

Diebold recommended decertification of its older version, which should force precincts to upgrade and eliminate the flaw. But the secretary of state's report notes flaws in the audit logs that will be harder to erase: wrongly recorded entry dates and times, and silent deletions of audit logs.

"It's nothing new," says Rebecca Mercuri, a security consultant who studied voting systems for her 1999 doctoral dissertation. "These are all security flaws that are well known in the industry. Why are they acting as if this is the first time they've heard this?" The audit log problems were documented in Bev Harris's 2004 book, *Black Box Voting* (blackboxvoting.org).

Mercuri explains that election software belongs to the class of problems known as "NP-complete," that is, problems computers cannot solve in a known amount of time. How much time have you got to test that a given voting system will function perfectly under all possible circumstances?

"What are people going to do about it?" she asks. "Say we fixed it when it's theoretically not possible to fix these things at any real level?"

So, it's not fair just to pick on Diebold. Last month, election officials in Clay county, Kentucky, were charged with conspiring to alter ballots cast on ES&S iVotronic election machines in recent elections. The key: interface design. In most cases, voters cast ballots by pressing a big red button labeled "VOTE." But some versions of the system require touching a "confirm vote" box on the screen to complete the ballot. It is alleged officials hid this fact from voters and would then "correct" and confirm the ballot after the voter had left. The officials have pleaded not guilty.

Matt Blaze, a security researcher at the University of Pennsylvania, writes in his blog that if this were a strategy, "it's a pretty elegant attack, exploiting little more than a poorly designed, ambiguous user interface, printed instructions that conflict with actual machine behavior, and public unfamiliarity with equipment that most citizens use at most once or twice each year. And once done, it leaves behind little forensic evidence to expose the deed."

But Diebold's current problems aren't limited to voting machines. More startling was the discovery of malware designed to attack its ATMs. Graham Cluley, a senior technology consultant for the security company Sophos, says the company found a sample in its archives.

"If [the malware] were planted on the version of Windows on those Diebold machines," Cluley says, "you could actually steal information from the cards being used on the device, and hackers with a specially crafted card would get a receipt with people's information." Diebold sent out a customer warning in January and provided a software update.

As in the Kentucky voting machine case, the attack on Diebold's ATMs requires inside access. "We're seeing more and more organized criminal gangs because of the money they can make," says Cluley, pointing out how difficult it would be to spot a legitimate maintenance engineer who's been bought off installing an extra patch off a USB stick in a back pocket.

For consumers, the problem is that both ATMs and voting machines are black-box technologies. You can count your cash and keep the receipt; but if someone else withdrew the money you can't prove it wasn't you. "It's the same with voting," Mercuri says. "You have no way to prove or disprove how you voted."

At least with voting, citizen groups are motivated to push for greater transparency. In the UK, Jason Kitcat, Green councilor for Brighton and Hove, on the south coast of England, organized volunteers to observe e-voting trials in the 2007 local government elections in England and Scotland on behalf of the Open Rights Group.

"We saw the same audit log issues," he says. "We know from a computer science point of view that making an audit log that can't be changed is impossible. But it seems as if there's a huge disconnect between people who are computer-science literate, and the people delivering the policy."

Besides, politicians like making uncontroversial decisions. Who could fault them for trusting a company that makes ATMs worldwide? Again, it comes back to humans.

"The folks who buy ATMs [bank managers] and voting machines [election officials] don't really want to pay for a facility that will make it easier for people to challenge them," says Ross Anderson, a professor of security engineering at Cambridge University, England.

"In the long run, of course, this ends up costing them more: fraud can lead to challenges that are systemic rather than local. Nevertheless, the purchasers may be rational. Most of the bank managers who bought crap ATM systems in the '80s are retired now — they got away with it. With voting machines, some vendors have been discredited in some countries, but lots of money has still been made."

That is, from us — the taxpayer and the bank customer. Kitcat says: "It is shocking that in this day and age this has been allowed to continue."