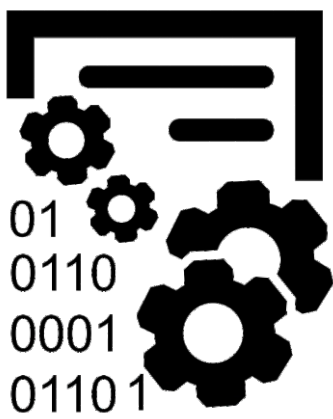


BITS AND BYTES

0
0 1
1 1 0 1



QUANTUM COMPUTING

QUANTUM COMPUTING IS ON A PATH OF ACCELERATING PUBLIC INTEREST DUE TO THE HOPE THAT NEW PRINCIPLES IN QUANTUM INFORMATION WILL IMPACT SOCIETY AS MUCH AS THE INFORMATION REVOLUTION AND MOORE'S LAW. WHILE THERE IS REASONABLE BASIS FOR QUANTUM COMPUTING BEING IMPORTANT, CURRENT PUBLIC EXPECTATIONS HAVE MOVED FAR BEYOND REALITY.

- THE FOUNDATION OF QUANTUM COMPUTING IS A UNIT CALLED THE QUBIT, THE BASIC UNIT OF INFORMATION IN A QUANTUM COMPUTER. MAKING QUBITS AND GETTING THEM TALK TO EACH OTHER IS A HARD TASK, BECAUSE THEY ARE TOUCHY AND EASILY GIVE UP THEIR QUANTUM-NESS WHEN IN CONTACT WITH THE OUTSIDE WORLD. CONNECTING THEM AND MAKING THEM WORK TOGETHER IS A HARDER TASK. VIJAYARAGHAVAN, A PROFESSOR AT THE TATA INSTITUTE OF FUNDAMENTAL RESEARCH (TIFR) IN MUMBAI, HAS MADE A THREE-QUBIT PROCESSOR WHERE EACH QUBIT IS CONNECTED TO EACH OF THE OTHER TWO QUBITS.
- IN TERMS OF THE NUMBER OF QUBITS, IT IS TRIVIAL. EARLY THIS YEAR, GOOGLE ANNOUNCED THAT IT HAD A QUANTUM PROCESSOR WITH 72 QUBITS, AND IBM HAD DEMONSTRATED A 50-QUBIT PROCESSOR LAST YEAR. BUT THEIR PROCESSOR ARCHITECTURES ARE DIFFERENT FROM THAT OF THE TIFR DEVICE. IN THE IBM-GOOGLE APPROACH, A QUBIT IS CONNECTED ONLY TO THE NEIGHBOURING QUBITS. IN THE TIFR DEVICE, EVERY QUBIT WILL BE CONNECTED TO EVERY OTHER QUBIT. IF VIJAYARAGHAVAN MANAGES TO SCALE HIS PROCESSOR TO MORE QUBITS, HE MAY HAVE A PROCESSOR THAT IS VERY EFFICIENT IN TRANSLATING ALGORITHMS.
- QUANTUM COMPUTERS ARE ENTIRELY DIFFERENT FROM THE SO-CALLED CLASSICAL MACHINES, AS THEY ARE CAPABLE OF SOLVING PROBLEMS THAT ARE IMPOSSIBLE FOR TODAY'S COMPUTERS. IN THIS SENSE, THEY ARE NOT SUPER VERSIONS OF TODAY'S COMPUTERS. A SUPERCOMPUTER, NO MATTER HOW FAST, CANNOT BREAK SECURITY CODES USED IN MILITARY AND BUSINESS COMMUNICATIONS. A QUANTUM COMPUTER CAN BREAK THEM IN MINUTES. IF, FOR EXAMPLE, SOMEONE IN THE WORLD DEVELOPS A QUANTUM COMPUTER, ALL OF TODAY'S SECURITY CODES BECOME WORTHLESS. WE WOULD THEN NEED TO DESIGN NEW ONES USING QUANTUM COMPUTERS.
- IN THE GLOBAL RACE TO BUILD QUANTUM COMPUTERS, INDIA HAS SO FAR BEEN PRESENT ONLY IN THEORY COMPARED TO US, CHINA AND THE HANDFUL OF OTHER EUROPEAN COUNTRIES THAT WERE SPENDING LARGE AMOUNTS OF MONEY. INDIA HAD NO NATIONAL PROGRAMME. IT HAD A NUMBER OF THEORISTS, BUT ONLY A FEW HAD BEEN TRYING TO BUILD A QUANTUM COMPUTING DEVICE.
- A FEW EXPERIMENTAL RESEARCH GROUPS STARTED EMERGING ABOUT FIVE YEARS AGO, AND SOME OF THEM HAVE MADE PROGRESS. NOW THE DEPARTMENT OF SCIENCE AND TECHNOLOGY (DST) WANTS TO GIVE THEM MORE MONEY, AS IT REALISED THAT QUANTUM COMPUTERS ARE ESSENTIAL TO TACKLE PROBLEMS THAT WILL DEVELOP IN THE FUTURE.

BETTER SOLUTIONS TO CURRENT PROBLEMS? WHAT PROBLEMS WILL QUANTUM COMPUTERS SOLVE BETTER THAN CLASSICAL COMPUTERS AND HOW MUCH WILL IT MATTER TO SOCIETY? THERE IS A WELL-STUDIED ALGORITHM FOR FACTORING NUMBERS THAT HAS IMPLICATIONS TO ENCRYPTION AND THERE ARE QUANTUM COMPUTING ALGORITHMS FOR OPTIMIZATION THAT COULD FIND SOLUTIONS CLOSE TO THE GLOBAL OPTIMUM THAN ANY ALGORITHM ON A CLASSICAL COMPUTER. ARTICLES CAN ADDRESS THE DEGREE TO WHICH SOCIETY MAY BE CHANGED BY THE RELATIVE IMPROVEMENT OFFERED BY SHIFTING FROM A CLASSICAL TO QUANTUM COMPUTING. FOR EXAMPLE, COULD A STOCKBROKER USING A QUANTUM COMPUTER BECOME MORE SUCCESSFUL THAN ONE JUST USING A CLASSICAL ONE BY PREDICTING STOCKS MORE ACCURATELY?

NEW APPLICATIONS QUANTUM COMPUTERS ARE BELIEVED CAPABLE OF SOLVING SOME PROBLEMS THAT ARE INTRACTABLE FOR TODAY'S COMPUTERS. SOME SUCH PROBLEMS ARE NOT CURRENTLY CONSIDERED IMPORTANT, BUT IT SEEMS OBVIOUS THAT THERE WILL BE NO BIG PROFITABLE COMPANIES SELLING SOLUTIONS TO SUCH PROBLEMS. HOWEVER, IF A QUANTUM COMPUTER CAN SOLVE A KNOWN BUT PREVIOUSLY INTRACTABLE PROBLEM, COULD COMPANIES EMERGE THAT SELL NEW, USEFUL PRODUCTS AND THEN GROW TO BE BIG AND PROFITABLE?

MANUFACTURING QUANTUM COMPUTERS HAVE BEEN DEMONSTRATED TO THE LEVEL OF 502,000 QUBITS, CREATING A PARALLEL WITH EARLY ELECTRONIC COMPUTERS' 50-2,000 RELAYS OR VACUUM TUBES. IN THIS PARALLEL, MOORE'S LAW AND OTHER EFFECTS BOOSTED THE NUMBER OF ACTIVE COMPONENTS BY A BILLIONFOLD IN LESS THAN A CENTURY. HOWEVER, THERE IS ONLY ONE EXAMPLE OF SUCH A LARGE IMPROVEMENT IN FACTOR, AND THE IMPROVEMENT DIDN'T COME FOR "FREE" BUT WAS HEAVY INVESTMENT IN THE DEVELOPMENT OF CURVED SURFACE SEMICONDUCTORS. ASSUMING QUANTUM COMPUTER PHYSICS IS SOUND, WHAT WOULD BE REQUIRED TO MOVE RESEARCH DEMONSTRATIONS TO COMMERCIAL PRODUCTS?

QUANTUM COMPUTER SOFTWARE ENGINEERING EARLY LANGUAGE FOR BOTH CLASSICAL AND QUANTUM COMPUTERS MERELY PROVIDED BOOKKEEPING ASSISTANCE FOR CONTROLLING THE UNDERLYING HARDWARE, SUCH AS ASSEMBLY LANGUAGE FOR CLASSICAL COMPUTERS AND GATE SEQUENCES FOR QUANTUM COMPUTERS. AS PROGRAMMING LANGUAGES FOR CLASSICAL COMPUTERS EVOLVED TO EMBRACE HIGHER PROGRAMMER PRODUCTIVITY THROUGH, FOR EXAMPLE, OBJECT ORIENTATION, DOMAIN SPECIFICITY, AND GRAPHIC PROGRAMMING METHODS. TO ACHIEVE QUANTUM SPEEDUP, QUANTUM ALGORITHMS MUST INVOKE ONE OF SEVERAL UNIQUELY QUANTUM FEATURES, SUCH AS QUBIT PHASE, INTERFERENCE, ENTANGLEMENT AND SO FORTH. HOW WILL QUANTUM COMPUTER SOFTWARE ENGINEERING TOOLCHAINS THAT IMPROVE PROGRAMMER PRODUCTIVITY FOR QUANTUM COMPUTERS EVOLVE TO ACHIEVE QUANTUM SPEEDUP?

QUANTUM MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE: THERE IS BOTH A THEORETICAL BASIS AND EXPERIMENTAL EVIDENCE THAT QUANTUM COMPUTERS CAN LEARN TRAINING SETS MORE EFFICIENTLY.



WRITTEN BY :
PROF. MR. Y. J. GAIKWAD (IF)
PROF. MRS. P. U. NEHETE (IF)