Report on Computer Science Colloquium Series

Chuang-Chieh Lin
Student ID: 893410010

April 18, 2005

1 Introduction

This report will focus on Professor Hsueh-I Lu, and Sheu and Pei-Yin Chen's speeches since I was mostly impressed by the concepts, results and research methods introduced by them. This report states my sentiments and opinions about these speeches. This report includes three subjects as follows. The first subject is "*An optimal algorithm for identifying a maximum-density segment*", which was given by Professor Hsueh-I Lu. The second subject is "*Introduction to Embedded Systems*", which was given by Professor Pei-Yin Chen. Among these speeches, I relish the first subject the most since this topic of research is strongly related to my research in computational biology and computer algorithms are my favorite.

2 An optimal algorithm for identifying a maximum-density segment

This speech was given by Professor Hsueh-I Lu on March 21. He is a associate professor in the department of Computer Science and Information Engineering in National Taiwan University now. I knew Professor Lu before and had a dinner with him about one year ago. He is too kind for me to think of he is a professor. He gave me some advices in doing research and suggest some plans for my career of research to to me. The content of this speech given by Professor Hsueh-I Lu is as follows.

”What do algorithm people do?” is his first question. From this question asked by him, we can know that maybe we have few speeches talking about algorithms, so most people are not interested in computer algorithms. His answer is that what algorithm people do is to *invent efficient recipes to solve combinatorial problems*. This sentence is fit to the keypoints. Consider the famous *factorization problem* whichc is a combinatorial problem. Given an positive integer N, if N is a prime number, output ***YES***; Otherwise, find a factorization of N. For example, if $N = 323264989793317$, the output to this factorization problem is ”18672511×17312347”. Actually we can easily find that it is more easy to design an instance to this problem than to solve it. For example, we can randomly give two positive large integers p and q and then we can get $N = p \times q$, then we obtain an instance to ask somebody. This problem is strongly related to cryptography systems, since the security of many encryption schemes is based upon the assumption that the factorization problem is difficult. How difficult is it? Well, finding an efficient recipe to the factorization of number is an OPEN PROBLEM. Why is it hard? Can’t we just find numbers among 1 and $\sqrt{N}$ and check if there exists a number $1 \leq x \leq n$ such that $N = xy$ where $y = \frac{N}{x}$? This method is correct but the time complexity is exponential. Why? Shouldn’t it be $O(N)$ and surely linear? Since N will be in binary representation, we can find that N needs ”$\lg N$” bits to be stored. Let $k = \lg N$ then we have $O(N) = O(2^k)$, which is exponetial with respect to k. Therefore, this method is not efficient.

When we talk about the encryption schemes, th RSA encryption scheme is undoubtedly the most famous among all encryption schemes. RSA is an abbreviation of the three authors *Rivest, Shamir* and *Adleman*. Their paper ”*A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Communications of the ACM, Vol. 21, pp.120-126, 1978*” accomplished this encryption system. They received the 2002 Turing Award in year 2003. This paper has only 7 pages.

Another hard problem called *PRIMES* is as follows. Given a number N, if N is a prime number then output ***YES***, otherwise output ***NO***. *PRIMES* is very like the factorization problem yet we don’t have to find the factorization of N is N is not a prime number. Finding a recipe to *PRIMES* had been also an open problem until Agarwal, Kayal, and Saxena solve it and published their result in August

6, 2002. This paper has only 9 pages! Now we can find that sometimes good research results are not necessarily complicated or long stories.

Professor Hsueh-I Lu and his student proposed an optimal algorithm for identifying a maximum-density segment. Their result was publish on *SIAM Journal on Computing*, which is very famous journal in computer science. The concept of their work is quite simple, too. The previous algorithm to solve the identifying a maximum-density segment problem is very complicated and the time complexity is of $O(n \log n)$. However, Professor Hsueh-I Lu and Kai-Min's approach is simple and the time complexity of their algorithm is of $O(n)$. Undoubtedly everyone should praise and appreciate their amazing work.

One of Professor Hsueh-I Lu's criteria for doing research is ”to make progress everyday”. This criteria becomes a new principle of our laboratory for doing research now. Everyday we work hard to reach this principle.

3 Introduction to Embedded Systems

Professor Pei-Yin Chen is an associate professor in Department of Computer Science and Information Engineering in National Cheng-Kung University now. His research is about SoC Embedded System Design, VLSI Chip Design, Image Compression and Fuzzy Control Applications. His speech in April 11 introduces the embedded systems to us. Since his speech is fundamental to me, I learned what an embedded system is and the difference between the traditional PC and an embedded system. Usually we design an embedded system for a special purpose, so this is the main difference between it and a PC. Nowadays, SoC means ”System on Chip”, which integrates a few component into a single chip. In the design of SoC, sometimes we have to consider the problem of power, the performance of integrating software component. Since the software component is important and it needs CSIE people to devote themselves in this work, our graduate or university students can find jobs in SoC or the embedded system design after they graduate. Sometimes we want to integrate many functions into a single chip, but it is expensive and the performance is not very good. Therefore it sounds like a dilemma in the design work. However, just like Professor Chen's opinion, the design work of embedded systems is decided by the demands and requirements. Each kinds of design work is valuable.

4 Acknowledgement and Suggestions

All speakers invited in this course are very charming and interesting. I think that everyone learns much and enlightened a lot. Here I want to express my appreciation for the teachers who were in charge of inviting and accommodating the speakers. Without your effort, we cannot enjoy these wonderful and spectacular speeches. Because of this class, we have chances to learn much more new knowledge and new concepts of research which aids in ourselves research.

I suggest that we may invite more speakers who do theoretical research. I think that theoretical materials are the most important elements in computer science, such as algorithms, mathematics, etc. I beliece that all the graduate students will reap no little benefit in a speech on a theoretical topic. It is not good that we can't endure any theoretical speech and want keep ourselves away from it every time. Computer science is a science talking about solving problems, so knowing and understanding mathematics and algorithms are very important.