* **Project 1** (Reading, HSP): algorithms for solvable groups and impossibility results for symmetric group
  + John Watrous. **Quantum algorithms for solvable groups**. *Proceedings of the 33rd ACM Symposium on Theory of Computing*, pages 60–67, 2001.
  + Negative results of Strong Fourier Sampling:
    - Cristopher Moore, Alexander Russell, Leonard J. Schulman, **The Symmetric Group Defies Strong Fourier Sampling**. *SIAM Journal on Computing*, 37(6): 1842-1864, 2008.
    - Sean Hallgren, Cristopher Moore, Martin Rötteler, Alexander Russell, Pranab Sen, **Limitations of quantum coset states for graph isomorphism**¸ *Journal of the ACM* 57(6): 34, 2010.
* **Project 2** (Reading, HSP): HSP for Dihedral group.   
  ***Taken by Russell Lai Wai Fu and Cheung Kam Fung*.**
  + Oded Regev, **Quantum Computation and Lattice Problems**. *SIAM Journal on Computing*, 33(3):738-760, 2004.
  + Greg Kuperberg, **A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem**, *SIAM Journal on Computing*, 35(1): 170-188, 2005.
  + Oded Regev, **A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space**, arXiv:quant-ph/ 0406151.
  + Greg Kuperberg, **Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem**, arXiv:1112.3333, 2011.
* **Project 3** (Research, query lower bound): Bound quantum query complexity by maximum influence. For a Boolean function , the influence of variable is defined as , where is chosen from uniformly at random, and is the string obtained from by flipping the -th bit. Recall that the quantum query complexity is at least for any nonzero Hermitian matrix . Prove the following conjecture (by constructing a and applying the above bound):

.

* *For background of the conjecture, see the following manuscript:* <http://www.cse.cuhk.edu.hk/~syzhang/papers/QQC_Influence.pdf>
* *For background of influence, see, for example, the online book* <http://analysisofbooleanfunctions.org/>
* Project 4 (Research, searching algorithm)   
  ***Taken by Junjie Ye***   
  One open problem in quantum searching algorithms is to pin down the quantum query complexity of the Triangle problem. In the problem, the input is the adjacency matrix of an -node graph , and the task is to decide whether contains an triangle. Using Grover’s search (on all possible triples of vertices), one gets an quantum algorithm using queries. Later development improved it to (<http://arxiv.org/abs/1210.1014>, SODA’13). Can you further improve it, or prove a lower bound better than ?
* Project 5 (Reading, communication complexity)  
  ***Taken by NG Tsz Ming and YIN Ho Fai Hoover  
  Also taken by Poon Chun Yeung and Sham Yik Hin***  
  Nonlocality is an interesting subject in quantum mechanics and here is a recent survey and a recent result on binary constraint games.
  + Harry Buhrman, Richard Cleve, Serge Massar, Ronald de Wolf. **Nonlocality and communication complexity**, *Reviews of Modern Physics*, Volume 82, 2010
  + Richard Cleve, Rajat Mittal. **Characterization of Binary Constraint System Games**, [arxiv/1209.2729](http://arxiv.org/abs/1209.2729)v3, 2013.
* Project 6 (Research, communication complexity)  
  ***Taken by*** ***Leung Chun Tat***   
  We proved that in the private-coin SMP model, the quantum communication complexity for is . Another interesting question is to consider structured inputs such as matrices. Suppose Alice’s input is a matrix and Bob’s input is another matrix . The function to compute is if , and if . (The rank is over .) In [LZ13], it was showed that the private-coin SMP quantum communication complexity satisfies that  
  The gap can be exponential when, e.g., . Can you improve either the lower or the upper bound above? (I’d conjecture that the upper bound is not tight. Btw, you can take if you like.)

[LZ13] Yang Liu, Shengyu Zhang. [Quantum and randomized communication complexity of XOR functions in the SMP model](http://www.cse.cuhk.edu.hk/~syzhang/papers/XorCC.pdf), ECCC, 2013.

* Project 7. (Reading, Lower bounds for quantum communication complexity.)   
  ***Taken by Hongyi Zhang***  
  We didn’t cover lower bounds for quantum communication complexity but it’s a very interesting subject. There is a nice survey with emphasis on norm-based methods.   
  [LS09] Troy Lee and Adi Shraibman, Lower bounds on communication complexity, *Foundations and Trends in Theoretical Computer Science*, 2009.
* Project 8. (Research, quantum communication complexity)  
  ***Taken by Tao Xin and Wang Yi***  
  We talked about a recent protocol [Z14] in Lecture 8. It’ll be great if the exponential dependence on the degree can be improved.   
  Bait 1: It may not be that hard (actually I didn’t put too much time on this yet).   
  Bait 2: If you can improve it, you’ll get a publication, likely in a top conference.   
  [Z14] Shengyu Zhang, Efficient quantum protocols for XOR functions, *Proceedings of the 25th Annual ACM-SIAM Symposium on Discrete Algorithms* (SODA), 2014, to appear.
* Project 9. (Reading, Fourier analysis)  
  ***Taken by Qin Liu***   
  Fourier analysis over is a well-studied subject with numerous applications in many areas in theoretical computer science, such as learning, testing, PCP, etc. A good book is the following one by O’Donnell. Read any four chapters of the book.  
  [O’D13] <http://www.contrib.andrew.cmu.edu/~ryanod/>