Project Zero Knowledge Proofs
Exercises 4

November 27, 2014

1 Commitment Schemes

1. Can you think of some other ways to commit the colours of the vertices of a graph in real life?

2. Can you think of ways to commit (in real life) more than one property of a vertex (color, adjacent vertices, name)?

2 Final Assignment (in groups)

The following problems are all NP-complete. Choose one of them and provide a Zero-Knowledge proof of knowing a witness. Show that your proof is indeed Zero-Knowledge and analyse its soundness and completeness errors. If you cannot find a zero-knowledge proof, argue why your methods fail. Present your (tried) solutions at the end of this course.

The problems are divided into two categories: Graphs and Puzzles. For the graphs, you need to find an algorithm that can be programmed. For the puzzles, try to find a real-life commitment scheme so that you can actually show your mother how smart you are (they work great at parties, too).

Graphs

- **Clique:** A graph contains a clique of size k if it contains a totally connected subgraph with at least k vertices. The verifier asks the prover: "Does graph G contain a clique of size k?"

- **Hamiltonian Cycle:** A Hamiltonian cycle though a graph is a path that visits each vertex exactly once, and ends at the same point it started. The verifier asks the prover: "Can you find a Hamiltonian cycle through the vertices of graph G?"

- **Vertex Cover:** A vertex cover of a graph is a subset of the vertices such that every edge is incident to at least one vertex in this subset. The verifier asks the prover: "Is there a vertex cover of G consisting of at most k vertices?"

Puzzles

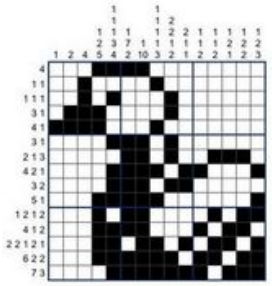
- **Sudoku on an $n^2 \times n^2$ grid:** This extension of the well-known 3×3 sudoku game asks to write the natural numbers $1, \ldots, n^2$ in each cell of an $n^2 \times n^2$ grid, in such a way that each column, row, and $n \times n$ block in the grid contains the numbers $1, \ldots, n^2$ exactly once. The puzzle has some numbers already filled in, the goal is to complete it.

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

In finding your zero-knowledge proof, think of the following:

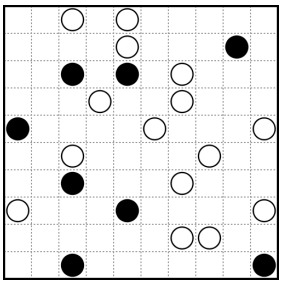
1. What are the requirements for a correct solution? What does the verifier need to check?
2. How can the prover commit his solution / the things the verifier needs to check?
3. How can the information the verifier gets be randomized, so the proof is zero-knowledge?

- **Nonogram (or Japanese Puzzle):** Played on an $n \times m$ grid with a sequence of numbers associated to each row and column. The numbers indicate the number of consecutive black squares on that specific row/column. The order in which the numbers appear is also the order of the blocks of black squares in that row/column. Different blocks of black squares are separated by at least one white square. The aim is to colour some squares in the grid black, such that the result is in agreement with the numbers given in each row and column. Usually an image appears when the puzzle is coloured correctly.



1. Consider the paper 'Cryptographic and Physical Zero-Knowledge Proof: From Sudoku to Nonogram' by Yu-Feng Chien and Wink-Kai Hon. Present their physical zero-knowledge proof, and prove theorem 4 of that paper (that is, prove the completeness and soundness errors, and the fact that the protocol is zero-knowledge).

- **Masyu:** This puzzle is played on an $n \times m$ grid. Squares can contain a white pearl, a black pearl, or be empty. The aim is to find a closed, non-intersecting path passing through every pearl. When the path crosses a black pearl, it has to turn 90 degrees, and it cannot turn immediately before or after the black pearl. When the path crosses a white pearl, it cannot turn, but it has to turn 90 degrees immediately before or after the white pearl.



In finding your zero-knowledge proof, think of the following:

1. What are the requirements for a correct solution? What does the verifier need to check?

2. How can the prover commit his solution / the things the verifier needs to check?

3. How can the information the verifier gets be randomized, so the proof is zero-knowledge?

- **Pick yourself:** Pick any puzzle from the paper 'A survey of NP-Complete Puzzles' by Kendall et al. and try to come up with a zero knowlegde proof for the puzzle. If you find a zero-knowledge proof, prove that it is zero-knowledge and give the completeness and soundness errors. If you cannot find a zero-knowledge proof, present you methods of finding one and explain why the protocols you tried do not work.