T-79.511 Special Course on Cryptology / Zero Knowledge: Selected comments on Lauri Tarkkala's "IP=PSPACE"

Mika Kojo

October 2, 2001

1 Introduction

In this note I shall shortly comment on the paper [?]. Overall I have very little to say, as the paper is a well written and indeed readable.

The paper [?] attempts to prove that **IP** $\subseteq$ **PSPACE** and **PSPACE** $\subseteq$ **IP**. Namely that interactive proofs can be used to prove anything in **PSPACE**. It is interesting to ask what does this mean in practice. What can be proven and what cannot?

Let us go through the paper [?] and consider few minor issues before concluding.

2 PSPACE and interactive proof systems

In interactive proof systems one has two parties the verifier and the prover. Both can be naturally viewed as Turing machines communicating over some shared tape. The exposition in [?] is accurate, although somewhat difficult to read for an algebraist like me. For example, giving a type

$$V : \Sigma^* \times \Sigma^* \times \Sigma^* \to \Sigma^* \cup \{\text{accept}, \text{reject}\}$$

gives little in terms of readability and semantics. I mention this because I have hard time finding other problems in the paper.

On the otherhand, the paper [?] does give semantics for the verifier and prover in somewhat dense way. Certainly it would be nice to know what ϵ means (I suspect it denotes empty string, naturally).

Finally, although I understand the computer scientist approach to mathematics it still annoys to read "interactive proofs systems with error probability 1/3". To me this sounds that you always have error probability 1/3, whatever you do.

3 IP $\subseteq$ PSPACE

The corresponding section in [?] produces a proof of the statement **IP** $\subseteq$ **PSPACE**. Apparently there are several proofs. It would be interesting to hear something about their differences.

Proof sketch that is given is readable. It would be good to use consistent terminology, like "well-formed" (instead of "well-founded") throughout.

4 PSPACE $\subseteq$ IP

This is the main part of the paper [?] it gives the arithmetization by Shen (instead of the one by Shamir).

In [?] it is somewhat difficult, at first, to follow Shen's arithmetization as nowhere it is indicated what is the domain. Namely, do we work with integers or over some other ring. Naturally, we must work over integers as becomes clear later. However, I would have liked to see this explicitly mentioned. For example, if integers were not be mandatory (as they are) then one could just as well work over $\mathbb{F}_2$ directly.

Basically the idea is to perform quantifier elimination. It is an interesting topic in itself. Nevertheless, the construction by Shen is quite natural and elegant.

The application of this arithmetization comes in the interactive protocol, say $\beta(\alpha)$, which performs a proof for one indeterminate and uses the protocol α to prove the rest. Actually the notation in this part is confusing. I have difficulty in understanding which arguments are fixed and which are not. For example, the step (6) of the protocol with $S(r, c_1, \dots, c_l) = s(r)$ is unclear. Are c_i fixed? Proving something like this is not very interesting if you want the backtracking to work, I think.

In the step (4), in the above mentioned protocol, it is unclear exactly what happens. Namely, what is send and by whom. This can be deduced from the exposition.

Finally, to my knowledge "interpolation theorem" doesn't state that there exists less than or equal to d solutions for univariate polynomials in a field. It is "fundamental theorem of algebra". I am not even sure whether e.g. Lagrange's interpolation theorem would imply that there cannot be more than d solutions. Of course, it is obvious in a sense, but the proofs (for the fundamental theorem of algebra, that is) that I know are not too obvious.

The rest is of course backtracking which is clear from the construction of the protocol. The most interesting point is fact that the field F used determines the error probability. Note that in [**?**] it is not specified which finite field to use. However, we see quite easily that the Shen's arithmetization produces integer coefficients and thus the only possible choice are the "prime" fields $\mathbb{F}_p$. Namely, reduction mod p yields the wished field F.

(It is true that some other number field works also, but then it is the characteristic of the field that matters. So $|F|$ would not necessary have anything to do with the error probability. Yes, this is a very minor point.)

5 Conclusion

I knew little about the topic a priori and [**?**] gave quite elegant exposition of the topic. Even I could follow it throughout. Minor typos and inconsistencies seem to exists here and there in the paper, but I would not care about them. The hardest part for me was to understand which variables were fixed in the interactive sub-protocol β and which were not.

I wish to insist that I did not find anything wrong in the paper.

References

[1] Lauri Tarkkala, T-79.511 Special Course on Cryptology / Zero Knowledge: IP=PSPACE, October 1, 2001, Draft.