Quantum Information and Computation, Vol. 9, No. 7&8 (2009) 0648–0656

ENTANGLEMENT-RESISTANT TWO-PROVER INTERACTIVE PROOF SYSTEMS AND NON-ADAPTIVE PIR'S

RICHARD CLEVE
David R. Cheriton School of Computer Science and Institute for Quantum Computing, University of Waterloo
200 University Ave. W., Waterloo, Ontario N2L3G1, Canada
and
Perimeter Institute for Theoretical Physics, 31 Caroline St. N.
Waterloo, Ontario N2L2Y5, Canada

DMITRY GAVINSKY[a]
NEC Labs America, 4 Independence Way, Suite 200
Princeton, New Jersey, 08540, United States

RAHUL JAIN[b]
Centre for Quantum Technologies and Department of Computer Science, National University of Singapore
3 Science Drive 2, Singapore 117543, Singapore

Received June 23, 2008
Revised April 6, 2009

We show that every language in NP is recognized by a two-prover interactive proof system with the following properties. The proof system is entanglement-resistant (i.e., its soundness is robust against provers who have prior shared entanglement), it has one round of interaction, the provers' answers are single bits, and the completeness-soundness gap is constant (formally, NP $\subseteq \oplus\mathrm{MIP}^*{}_{1-\varepsilon,1/2+\varepsilon}[2]$, for any ε such that $0 < \varepsilon < 1/4$). Our result is based on the "oracularizing" property of a particular private information retrieval scheme (PIR), and it suggests that investigating related properties of other PIRs might bear further fruit.

Keywords: Quantum computing, interactive proof systems, entanglement
Communicated by: I Cirac & B Terhal

1 Introduction

Properties of interactive proof systems have been shown to change in fundamental ways when the underlying setting changed from classical to quantum information. The first result along these lines was discovered by Watrous [19], and several subsequent results have occurred (see, for example, the survey paper [20] and references therein).

The present paper falls within the scope of multi-prover interactive proof systems (MIPs), that were first proposed (in the classical setting) by Ben-Or *et al.* [2]. Roughly speaking, the scenario is that a polynomial-time bounded verifier interacts with several provers whose

[a]Research done while the author was at the David R. Cheriton School of Computer Science and Institute for Quantum Computing, University of Waterloo, Canada.
[b]Research done while the author was at the David R. Cheriton School of Computer Science and Institute for Quantum Computing, University of Waterloo, Canada.

computational power is unlimited, subject to not being able to communicate with one another once the protocol starts. Such a system recognizes a language L if and only if: (a) whenever $x \in L$, there exists a strategy for the provers that convinces the verifier that this is the case (completeness); (b) whenever $x \notin L$, whatever strategy the provers employ, they will not convince the verifier that $x \in L$ (soundness). Usually some error probability is allowed, and it is required that the gap between the acceptance probabilities of the verifier in cases (a) and (b) be at least constant.

The class of languages having such proof systems is referred to as MIP. In a series of fundamental results [1, 9] it was discovered, somewhat surprisingly, that MIP = NEXP (the class of languages recognized in non-deterministic exponential time).

It has been noticed by Cleve *et al.* [4] that in a quantum-mechanical world the provers, even when they are not able to communicate, can use shared quantum entanglement in order to increase the probability that the verifier accepts some instances outside the language. Indeed, in [4] it has been demonstrated that some classically-valid MIP systems are no longer valid when shared entanglement is allowed.

The power of MIPs with entanglement remains poorly understood. In particular, as far as we currently know, it can be the case that the class of languages recognized by MIPs with entanglement is a subset of, a superset of, the same as, or incomparable to NEXP.

In the classical scenario, the strength of MIPs intuitively stems from the "oracularizing" property of two non-communicating provers. Roughly speaking, this means that the verifier can force one of the provers to answer non-adaptively (i.e., to behave like an oracle). Direct application of the same technique to the case of entangled provers fails [4].

In this paper we give a new technique for oracularizing provers, which is based on the properties of particular Private Information Retrieval schemes (PIRs). A PIR is a scheme that enables information to be obtained from a database having multiple servers, without revealing to any individual server what information is being queried (cf. [3, 10]).

Intuitively, this seems like a natural approach to oracularizing provers in an MIP protocol: if the servers have no idea what was queried in the past, how can they make their answers adaptive? Observe that the property of non-adaptiveness is operationally different from that of privacy, as required by the definition of a PIR.[c] Non-adaptiveness can be viewed as an additional requirement to a scheme (trivial examples can be given of valid PIRs that are not non-adaptive).

We show that some PIRs are inherently non-adaptive. That is, the servers that constitute a PIR cannot collaborate in order to make their answers satisfy certain properties that non-trivially depends on the previous queries. Moreover, this remains true even if the servers share quantum entanglement.

Using this approach, we show that the languages in NP are recognized by certain types of proof systems with entangled provers, which we denote by $\oplus$MIP*[2]. These proof systems are closely related to the classical proof systems $\oplus$MIP[2], where the verifier makes one query of polynomial length to each of 2 provers and receives a binary answer to each query. The verifier's acceptance condition is a function of the queries he made, his private coins and the

[c] This distinction is reminiscent of the distinction between malleable cryptography and non-malleable cryptography [6]. For example, a crypto-system may be immune against attacks aiming to deduce x from its encryption, and nevertheless it may be possible to construct an encryption of y that is somehow related to x.

XOR of the answers. An $\oplus$MIP*[2] proof system is an $\oplus$MIP[2] system with allowed shared entanglement between the provers.

It is known ([11]) that $\oplus$MIP[2] = NEXP.[d] On the other hand, it has been shown recently in [13] that $\oplus$MIP* [2] is a subset of PSPACE (the class of languages recognizable using polynomial space). Therefore, NEXP is not contained in $\oplus$MIP*[2], unless NEXP = PSPACE (as opposed to a widely believed conjecture). Nevertheless, our technique demonstrates the potential viability of the general approach of using PIRs as "oracularizing tools" in the MIP setting.

1.1 Related work

Recently (independently to our work and using different techniques) several multi-prover systems have been found that allow shared entanglement between the provers.

Ito *et al.* [12] constructed three-prover one-round entanglement-immune systems with single-bit answers that (1) recognize NP with inverse-polynomial gap between completeness and soundness parameters; (2) recognize NEXP with inverse-exponential gap between completeness and soundness parameters.

In earlier work, Kempe *et al.* [14] gave one-round entanglement-immune proof systems for NP (with inverse-polynomial gap) and for NEXP (with inverse-exponential gap) that (1) consist of two provers but requires a quantum verifier; (2) consists of three provers.

2 Preliminaries

2.1 Notation

For $s, t \in \{0,1\}^m$, let $s \cdot t \in \{0,1\}$ denote the inner product modulo 2 of s and t, and $s \oplus t \in \{0,1\}^m$ denote the bit-wise exclusive-or of s and t. For $j \in \{1, 2, \ldots, m\}$, let $e_j \in \{0,1\}^m$ denote the characteristic vector of $\{j\}$, which is 1 in coordinate j and 0 in all other coordinates.

2.2 The class $\oplus$MIP$^*{}_{q,p}$[2]

Let $0 \leq p < q \leq 1$. A language L is said to be in the language class $\oplus$MIP$^*{}_{q,p}$[2] if it has a two-prover protocol of the following form. Let $x \in \{0,1\}^n$ be the input received by the provers P_1 and P_2, who share prior entanglement, and the verifier V.

1. V generates messages s and t and a private[e] string r. The strings (s, t, r) are chosen from a joint distribution which is samplable in time polynomial in n. V then sends s, t to P_1 and P_2 respectively.

2. P_1 and P_2 (after possibly making some measurements on their parts of the shared entangled state) respond with bits a and b, respectively.

3. V accepts x if and only if $a \oplus b = f_x(s, t, r)$, where f_x is computable in time polynomial in n.

The protocol must satisfy the following completeness and soundness properties.

[d] In this paper we will use the same notation to denote a proof system and the class of languages it recognizes, as it is customary in the complexity theory.

[e] This is a string that verifier V, keeps to himself and does not send to any of the provers; in this sense we refer to it as the private string. He uses this string later though in the final acceptance decision.

Completeness: If $x \in L$ then there exists a strategy for provers P_1 and P_2 such that V accepts with probability at least q.

Soundness: If $x \notin L$ then, for all strategies of provers P_1 and P_2, V accepts with probability at most p.

2.3 Håstad's 3-query PCP

Let $L \in$ NP and $\varepsilon \in (0, 1/4)$. Håstad [11] showed that there exists a Probabilistically Checkable Proof (PCP) system for L of the following form. There is a proof verification procedure $V_{\mathrm{PCP}}(L)$ that, for any n-bit string x (n large enough depending on ε), takes an m-bit string w as input (where m is polynomial in n) and accepts or rejects w as a certificate of $x \in L$ based on the parity of three bits of w as follows. $V_{\mathrm{PCP}}(L)$ probabilistically generates distinct $i, j, k \in \{1, 2, \ldots, m\}$ and $\delta \in \{0, 1\}$, from a polynomial time (in n) samplable joint distribution θ, and accepts if and only if $w_i \oplus w_j \oplus w_k = f_x(i, j, k, \delta)$, where function f_x is computable in time polynomial in n. The completeness and soundness properties of the PCP are as follows.

Completeness: For all $x \in L$, there exists a witness string $w \in \{0, 1\}^m$ such that $V_{\mathrm{PCP}}(L)$ accepts w with probability at least $1 - \varepsilon$.

Soundness: For all $x \notin L$, for all $w \in \{0, 1\}^m$, $V_{\mathrm{PCP}}(L)$ accepts w with probability at most $\frac{1}{2} + \varepsilon$.

2.4 Transversal XOR games

Let m, l be positive integers. A transversal XOR game $G(g, \pi)$, specified by a function $g : \{0, 1\}^m \times \{0, 1\}^l \to \{0, 1\}$ and a distribution π on $\{0, 1\}^m \times \{0, 1\}^l$, is an interactive game between a referee $\mathcal{R}$, and two parties $\mathcal{A}$ and $\mathcal{B}$ sharing entanglement. The operation of the game is as follows.

1. $\mathcal{R}$ generates $(z, r) \in \{0, 1\}^m \times \{0, 1\}^l$ according to the distribution π. The string r is a private string of $\mathcal{R}$, which is not send to the provers, but is used later while accepting or rejecting. $\mathcal{R}$ produces two shares, namely s and t, of z by generating $s \in \{0, 1\}^m$ uniformly and independently of z and setting $t = s \oplus z$. $\mathcal{R}$ then sends s to $\mathcal{A}$ and t to $\mathcal{B}$.

2. $\mathcal{A}$ and $\mathcal{B}$ produce bits a and b respectively, possibly by making measurements on their parts of the shared quantum state, and send them to $\mathcal{R}$.

3. $\mathcal{A}$ and $\mathcal{B}$ win as a team if and only if $a \oplus b = g(s \oplus t, r)$; otherwise $\mathcal{R}$ wins.

The transversal XOR games that we consider are a generalization of the games considered by Linden *et al.* [18]. In these games, the referee $\mathcal{R}$ does not generate the private string r. We show the following result about transversal XOR games that we will need later. It is a relatively straightforward generalization of a result in [18], where the corresponding result was shown without involving the sting r. We provide its proof in Appendix 1.

Lemma 1 *Let $G(g, \pi)$ be a transversal XOR game specified by $g : \{0, 1\}^m \times \{0, 1\}^l \to \{0, 1\}$ and the distribution π on $\{0, 1\}^m \times \{0, 1\}^l$. Let a, b, s, t, r be as in the description above. A*

strategy that maximizes $(\mathcal{A}, \mathcal{B})$*'s probability of winning, that is* $\Pr[a \oplus b = g(s \oplus t, r)]$*, does not use any entanglement and is of the following form. For some* $u \in \{0,1\}^m$ *and* $\gamma \in \{0,1\}$ *(that depend on* g *and* π*),* $\mathcal{A}$ *responds with* $a = (u \cdot s) \oplus \gamma$ *and* $\mathcal{B}$ *responds with* $b = u \cdot t$*.*

3 Main result: NP $\subseteq \oplus$MIP*[2]

Our main result is as follows.

Theorem 1 *Let* $\varepsilon \in (0, 1/4)$ *be a constant and let* $L \in$ NP*. Then* $L \in \oplus\text{MIP}^*{}_{1-\varepsilon,1/2+\varepsilon}[2]$*.*

Proof. Let $\varepsilon \in (0, 1/4)$ be a constant and let $L \in$ NP. Recall the PCP procedure $V_{\text{PCP}}(L)$ defined previously. Consider the following $\oplus$MIP*[2] protocol $\mathcal{P}$ for L.

Protocol $\mathcal{P}$: On receiving input x ($|x| = n$), V interacts with provers P_1 and P_2 as follows.

1. V simulates $V_{\text{PCP}}(L)$ in the generation of $i, j, k \in \{1, 2, \ldots, m\}$ and $\delta \in \{0, 1\}$.
2. V chooses $s \in \{0,1\}^m$, uniformly distributed and independent of i, j, k, δ, and sets $t = s \oplus e_i \oplus e_j \oplus e_k$.
3. V sends s to P_1 and t to P_2, receiving one-bit answers a and b from them respectively.
4. V accepts if and only if $a \oplus b = f_x(i, j, k, \delta)$.

It is easily seen that $\mathcal{P}$ is a valid $\oplus$MIP*[2] protocol. It remains to show that $\mathcal{P}$ satisfies the desired completeness and soundness properties.

Completeness:

If $x \in L$ then we know from the PCP procedure $V_{\text{PCP}}(L)$ (assuming n is large enough) that there exists a PCP-witness $w \in \{0,1\}^m$ such that $V_{\text{PCP}}(L)$ accepts w with probability at least $1 - \varepsilon$. Consider the strategy in which P_1, on receiving s from V, sends back to V the bit $a = w \cdot s$, and P_2, on receiving t from V, sends back to V the bit $b = w \cdot t$. Now,

$$\begin{aligned} a \oplus b &= w \cdot (s \oplus t) \\ &= w \cdot (e_i \oplus e_j \oplus e_k) \\ &= w_i \oplus w_j \oplus w_k. \end{aligned}$$

Therefore V accepts whenever $V_{\text{PCP}}(L)$ accepts the PCP string w, and hence the probability of acceptance of V is at least $1 - \varepsilon$.

Soundness:

Recall the definition of transversal XOR games mentioned previously. In protocol $\mathcal{P}$, the verifier on receiving x can be thought of as playing (as referee $\mathcal{R}$) a transversal XOR game $G(g, \pi)$ with the provers P_1, P_2 (as players $\mathcal{A}, \mathcal{B}$ respectively) by setting $z = e_i \oplus e_j \oplus e_k$, $r = \delta$, $\theta = \pi$ and $g : \{0,1\}^m \times \{0,1\} \to \{0,1\}$ be such that $g(e_i \oplus e_j \oplus e_k, \delta) = f_x(i, j, k, \delta)$.

Let $x \notin L$. From Lemma 1 a strategy for the provers in which they are trying to maximize the acceptance probability of the verifier V is as follows. P_1 and P_2 ignore the entanglement and for some $u \in \{0,1\}^m$ and $\gamma \in \{0,1\}$, P_1 outputs $a = (u \cdot s) \oplus \gamma$ and P_2 outputs $b = u \cdot t$.

It can be easily shown that $\Pr[V \text{ accepts } x] = \Pr[a \oplus b = g(s \oplus t, \delta)] \leq 1/2 + \varepsilon$ as follows. Consider the following PCP witness w. For all $j \in \{1, 2, \ldots, m\}$, set $w_j = u_j \oplus \gamma$. Note that this witness satisfies

$$\begin{aligned} w_i \oplus w_j \oplus w_k &= u_i \oplus u_j \oplus u_k \oplus \gamma \\ &= u \cdot (e_i \oplus e_j \oplus e_k) \oplus \gamma \\ &= u \cdot (s \oplus t) \oplus \gamma \\ &= a \oplus b. \end{aligned}$$

Combining this with the fact that $f_x(i, j, k, \delta) = g(s \oplus t, \delta)$ enables us to conclude that

$$\Pr[a \oplus b = g(s \oplus t, \delta)] = \Pr[w_i \oplus w_j \oplus w_k = f_x(i, j, k, \delta)] \leq \frac{1}{2} + \varepsilon.$$

The last inequality comes from the soundness property of the PCP procedure $V_{\mathrm{PCP}}(L)$. Thus $\Pr[V \text{ accepts } x]$ in the protocol $\mathcal{P}$ is at most $\frac{1}{2} + \varepsilon$ and hence the soundness property is satisfied. □.

4 Concluding remarks

In this work, we have used a basic PIR scheme to construct a protocol that is robust against cheating provers who share entanglement. Since the PIR construction that we use requires polynomial-length questions from the verifier, we are only able to capture the class NP. This naturally suggests an investigation of other, more sophisticated, PIR schemes for constructing other protocols that may be robust against provers that share entanglement.

In our proof system, the completeness and soundness errors are not exponentially small, because these parameters arise from the PCP scheme used by Håstad [11]. However, we can apply the proof system a constant number of times in parallel to make the completeness and soundness errors arbitrarily small constants (by applying the direct-product result of [5]). Note that, in so doing, the size of each prover's answer increases in proportion to the number of repetitions.

Recently it has been demonstrated that $\oplus\mathrm{MIP}^*[2] \subseteq \mathrm{PSPACE}$ [13], and combined with our result this gives $\mathrm{NP} \subseteq \oplus\mathrm{MIP}^*[2] \subseteq \mathrm{PSPACE}$. Closing the gap between the two bounds is a natural open problem.

Acknowledgments

We thank the referees for providing useful comments for improving the presentation of the paper. This research was supported in part by Canada's NSERC, CIFAR, MITACS, and the U.S. ARO/DTO.

References

1. L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.
2. M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: how to remove intractability assumptions. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 113–131, 1988.
3. B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan. Private information retrieval. *Journal of the ACM*, 41–50, 1995.

4. R. Cleve, P. Høyer, B. Toner, J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th IEEE Conference on Computational Complexity*, pages 236–249, 2004.
5. R. Cleve, W. Slofstra, F. Unger and S. Upadhyay. Perfect Parallel Repetition Theorem for Quantum XOR Proof Systems. In *Proceedings of the Twenty-Second Annual IEEE Conference Computational Complexity*, pages 109-114, 2007.
6. D. Dolev, C. Dwork and M. Naor. Non-malleable cryptography. *SIAM Journal on Computing* 30(2):391–437, 2000.
7. U. Feige. On the success probability of two provers in one-round proof systems. In *Proceedings of the Sixth Annual Conference on Structure in Complexity Theory*, pages 116–123, 1991.
8. U. Feige and L. Lovász. Two-prover one-round proof systems: their power and their problems. In *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, pages 733–744, 1992.
9. L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. *Theoretical Computer Science*, 134:545–557, 1994.
10. W. Gasarch. A survey on private information retrieval. *Bulletin of the EATCS*, 82:72–107, 2004.
11. J. Håstad. Some optimal inapproximability results. *Journal of the ACM*, 48(4):798–859, 2001.
12. T. Ito, H. Kobayashi, D. Preda, X. Sun, A.C.-C. Yao Generalized Tsirelson Inequalities, Commuting-Operator Provers, and Multi-Prover Interactive Proof Systems. In *Proceedings of the 23rd IEEE Conference on Computational Complexity*, 2008. Also at arXiv:0712.2163.
13. R. Jain, S. Upadhyay, J. Watrous. Two-message quantum interactive proofs are in PSPACE. Manuscript in preparation. Personal communication. 2009.
14. J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled games are hard to approximate. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, 2008. Also at arXiv:0704.2903.
15. J. Kempe, O. Regev, B. Toner. The Unique Games Conjecture with Entangled Provers is False. In *Proceedings of the 49th Annual Symposium on Foundations of Computer Science*, 2008. Also at arXiv:0710.0655, 2007.
16. A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 608–617, 2000.
17. H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3):429–450, 2003.
18. N. Linden, S. Popescu, A. J. Short, and A. Winter. Quantum nonlocality and beyond: Limits from nonlocal computation. *Phys. Rev. Lett.* 99, 180502, 2007.
19. J. Watrous. PSPACE has constant-round quantum interactive proof systems. In *Theoretical Computer Science*, 292(3):575–588, 2003. Extended abstract in *Proceedings of the Fortieth Annual Symposium on Foundations of Computer Science*, pages 112–119, 1999.
20. J. Watrous Quantum Computational Complexity. arXiv:0804.3401, 2008.

Appendix A Proof of Lemma 1

Our proof is along the lines of the proof of Linden et al. [18]. In the transversal XOR game $G(g, \pi)$ (as defined in Section 2.4), let players $\mathcal{A}$ and $\mathcal{B}$ share a pure quantum state $|\phi\rangle$ between them. It can be seen via standard arguments, which we will not get into here, that the shared state can be assumed to be pure without loss of generality. Let Z, R be a pair of random variables jointly distributed according to π. Here R represents the private random string of the referee $\mathcal{R}$ in the game $G(g, \pi)$. Let $S \in \{0,1\}^m$ be a random variable corresponding to the string sent by the referee $\mathcal{R}$ to player $\mathcal{A}$. Let $T \stackrel{\triangle}{=} S \oplus Z$ be the string sent by $\mathcal{R}$ to player $\mathcal{B}$. From the properties of the transversal XOR game $G(g, \pi)$, S is uniformly distributed and independent of (Z, R). Let A, B represent the random variables corresponding to the answers

by $\mathcal{A}$ and $\mathcal{B}$ respectively. It is well-known (and can be verified by direct calculations) that $\Pr[g(z,r) = A \oplus B \mid (S,Z,R) = (s,z,r)]$ can be expressed without loss of generality as:

$$\Pr[g(z,r) = A \oplus B \mid (S,Z,R) = (s,z,r)] = \frac{1}{2}(1 + (-1)^{g(z,r)} \langle \phi | A_s \otimes B_{s \oplus z} | \phi \rangle),$$

where $A_s, B_{s \oplus z}$ are Hermitian operators with eigenvalues in $\{-1, 1\}$ (which are also sometimes referred to as observables). Therefore we have,

$$\begin{aligned}
\Pr[\mathcal{R} \text{ accepts}] &= \sum_{s,z,r} \Pr[(S,Z,R) = (s,z,r)] \Pr[g(z,r) = A \oplus B \mid (S,Z,R) = (s,z,r)] \\
&= \sum_{s,z,r} \Pr[(S,Z,R) = (s,z,r)] \cdot \frac{1}{2}(1 + (-1)^{g(z,r)} \langle \phi | A_s \otimes B_{s \oplus z} | \phi \rangle) \\
&= \frac{1}{2} + \sum_{s,z,r} \Pr[(S,Z,R) = (s,z,r)] \cdot \frac{1}{2}(-1)^{g(z,r)} \langle \phi | A_s \otimes B_{s \oplus z} | \phi \rangle) \\
&= \frac{1}{2} + \sum_{s,z} \frac{1}{2^n} (\sum_{r} \Pr[(R,Z) = (r,z)] \cdot \frac{1}{2}(-1)^{g(z,r)}) \langle \phi | A_s \otimes B_{s \oplus z} | \phi \rangle.
\end{aligned}$$

Here the last equality follows since S is uniformly distributed and independent of (Z,R). Now define,

$$\begin{aligned}
\theta_z &= \sum_r \Pr[(R,Z) = (r,z)] \cdot \frac{1}{2}(-1)^{g(z,r)} \\
|\alpha\rangle &= \frac{1}{\sqrt{2^n}} \sum_s (A_s \otimes I \otimes I)(|\phi\rangle \otimes |s\rangle) \\
|\beta\rangle &= \frac{1}{\sqrt{2^n}} \sum_t (I \otimes B_t \otimes I)(|\phi\rangle \otimes |t\rangle) \\
\Phi &= \sum_{s,z} \theta_z |s\rangle\langle s \oplus z|.
\end{aligned}$$

In the definitions of $|\alpha\rangle$ and $|\beta\rangle$ above, only the last identity acts on $|s\rangle, |t\rangle$ respectively. Note that $|\alpha\rangle, |\beta\rangle$ are unit vectors and Φ is Hermitian. Using the definitions above we have (below identity I acts on the Hilbert space corresponding to $|\phi\rangle$),

$$\begin{aligned}
\Pr[\mathcal{R} \text{ accepts}] &= \frac{1}{2} + \sum_{s,z} \frac{1}{2^n} \theta_z \langle \phi | A_s \otimes B_{s \oplus z} | \phi \rangle \\
&= \frac{1}{2} + \langle \alpha | (I \otimes \Phi) | \beta \rangle \\
&\leq \frac{1}{2} + ||\langle \alpha ||_2 ||(I \otimes \Phi)||_\infty ||| \beta \rangle ||_2 \\
&= \frac{1}{2} + ||(I \otimes \Phi)||_\infty \\
&= \frac{1}{2} + ||\Phi||_\infty.
\end{aligned}$$

Above $||\Phi||_\infty$ represents the highest singular value of Φ and since Φ is Hermitian it means the highest modulus eigenvalue.

Below we show that the eigenvectors of Φ are precisely the Hadamard vectors $|u\rangle = \sum_{v\in\{0,1\}^n}(-1)^{u\cdot v}|v\rangle$ (for $u \in \{0,1\}^m$) with eigenvalues $\lambda_u = \sum_z (-1)^{u\cdot z}\theta_z$. This can be calculated as,

$$\begin{aligned}
\Phi|u\rangle &= (\sum_{s,z}\theta_z|s\rangle\langle s\oplus z|)(\sum_{v\in\{0,1\}^n}(-1)^{u\cdot v}|v\rangle) \\
&= \sum_{s,z}(-1)^{u\cdot(s\oplus z)}\theta_z|s\rangle \\
&= (\sum_z(-1)^{u\cdot z}\theta_z)\sum_s(-1)^{u\cdot s}|s\rangle \\
&= \lambda_u|u\rangle.
\end{aligned}$$

Next we show that there exists a classical strategy by $\mathcal{A}$ and $\mathcal{B}$ such that $\Pr[\mathcal{R} \text{ accepts}] = \frac{1}{2} + ||\Phi||_\infty$ and we will be done. Let $|w\rangle$ be the eigenvector of Φ corresponding to the highest modulus eigenvalue, that is $|\lambda_w| = ||\Phi||_\infty$. Let $\gamma = 0$ if $\lambda_w \geq 0$ and 1 otherwise. Now let $\mathcal{A}$ send back $(w\cdot s)\oplus\gamma$ on receiving string s and let $\mathcal{B}$ send back $(w\cdot t)$ on receiving string t. Then we see that,

$$\begin{aligned}
\Pr[\mathcal{R} \text{ accepts}] &= \sum_{s,z,r}\Pr[(S,Z,R)=(s,z,r)]\Pr[g(z,r)=(w\cdot s)\oplus\gamma\oplus(w\cdot(s\oplus z))] \\
&= \sum_{s,z,r}\Pr[(S,Z,R)=(s,z,r)]\Pr[g(z,r)=(w\cdot z)\oplus\gamma] \\
&= \sum_{s,z,r}\Pr[(S,Z,R)=(s,z,r)](\frac{1}{2}+\frac{1}{2}(-1)^{g(z,r)+(w\cdot z)+\gamma}) \\
&= \frac{1}{2}+\sum_{s,z,r}\Pr[(S,Z,R)=(s,z,r)]\cdot\frac{1}{2}\cdot(-1)^{g(z,r)+(w\cdot z)+\gamma} \\
&= \frac{1}{2}+\sum_{z,r}\Pr[(Z,R)=(z,r)]\cdot\frac{1}{2}\cdot(-1)^{g(z,r)+(w\cdot z)+\gamma} \\
&= \frac{1}{2}+\sum_z\left(\sum_r\frac{1}{2}\cdot\Pr[(Z,R)=(z,r)]\cdot(-1)^{g(z,r)}\right)(-1)^{(w\cdot z)+\gamma} \\
&= \frac{1}{2}+\sum_z\theta_z\cdot(-1)^{(w\cdot z)+\gamma} \\
&= \frac{1}{2}+|\lambda_w| = \frac{1}{2}+||\Phi||_\infty.
\end{aligned}$$

□.