MIP* = RE Analysis

David Kravets
University of Maryland,
Baltimore County
CMSC 499

Abstract— An analysis of the MIP* = RE proof, including an annotated bibliography of a portion of the concepts needed for understanding this proof.

This paper contains mostly definitions, summaries, and information that is derived from the source material cited. This paper can be used as a quick reference for information related to MIP=RE

I. Introduction

This paper will be examining topics in classical and quantum game theory, physics, computing, and mathematics. The goal is to present a list of important concepts needed for in order to understand and analyze the paper MIP* = RE [0]. It is claimed that the class MIP* of languages that can be decided by a classical verifier interacting with multiple all-powerful quantum provers sharing entanglement is equal to the class RE of recursively enumerable languages. [0]

It should be predicated that MIP* = RE relies on many fundamental assumptions in theoretical physics, mathematics, and computing. The assumption of nonlocal games with provers being non-logarithmic in complexity (PCP theorem proven incorrect?), and a fundamental assumption that P ≠ NP.

II. Game Theory

Cooperative / non-cooperative

A game is *cooperative* if the players are able form binding commitments externally enforced. A game is *non-cooperative* if players cannot form alliances or if all agreements need to be self-enforcing .[7]

Cooperative games are often analyzed through the framework of *cooperative game theory*, which focuses on predicting which coalitions will form, the joint actions that groups take, and the resulting collective payoffs. It is opposed to the traditional *non-cooperative game theory* which focuses on predicting individual players' actions and payoffs and analyzing Nash equilibria.[8][9]

Symmetric/ asymmetric

A symmetric game is a game where the payoffs for playing a particular strategy depend only on the other strategies employed, not on who is playing them. That is, if the identities of the players can be changed without changing the payoff to the strategies, then a game is symmetric. Many of the commonly studied 2×2 games are symmetric. The standard representations of chicken, the prisoner's dilemma, and the stag hunt are all symmetric games. Some scholars would consider certain asymmetric games as examples of these games as well. However, the most common payoffs for each of these games are symmetric.

Zero sum / non zero sum

Zero-sum games are a special case of constant-sum games in which choices by players can neither increase nor decrease the available resources. In zero-sum games, the total benefit goes to all players in a game, for every combination of strategies, always adds to zero (more informally, a player benefits only at the equal expense of others).[10] Poker exemplifies a zero-sum game (ignoring the possibility of the house's cut), because one wins exactly the amount one's opponents lose. Other zero-sum games include matching pennies and most classical board games including Go and chess.

Simultaneous/ sequential

Simultaneous games are games where both players move simultaneously, or instead the later players are unaware of the earlier players' actions (making them effectively simultaneous).

Sequential games (or dynamic games) are games where later players have some knowledge about earlier actions. This need not be perfect information about every action of earlier players; it might be very little knowledge. For instance, a player may know that an earlier player did not perform one particular action, while they do not know which of the other available actions the first player actually performed.

Quantum

Low degree:

PCP: the PCP Theorem says that it is *NP*-hard to approximate the classical value of a nonlocal game (i.e. the maximum winning probability of classical players) to within constant additive accuracy (say +- 1/10). Thus, assuming that *P* is not equal to *NP*, we shouldn't expect a polynomial-time algorithm for this. [1]

In 1955, mathematician John Nash wrote a letter to the NSA, where he speculated that cracking a sufficiently complex code would require time exponential in the length of the key.[5] If proved (and Nash was suitably skeptical) this would imply what is now called P ≠ NP, since a proposed key can easily be verified in polynomial time. Another mention of the underlying problem occurred in a 1956 letter written by Kurt Gödel to John von Neumann. Gödel asked whether theorem-proving could be solved in quadratic or linear time and pointed out one of the most important consequences—that if so, then the discovery of mathematical proofs could be automated. [6]

Quantum Games

Nonlocal games:

The most famous example of a nonlocal game is the CHSH game: in this game, the verifier sends a uniformly random bit x to Alice (who responds with a bit a) and a uniformly random bit y to Bob (who responds with a bit b). The players win if $a \oplus b = x \wedge y$ (in other words, the sum of their answer bits is equal to the product of the input bits modulo 2). [1]

MIP = NEXP

Definition 1. NP is a class of language L such that there exists a poly time verifier V with

- For any $x \in L$, $|x| = n$, there exists a proof $\Pi \in \{0, 1\}$ poly(n) such that $V (x, \Pi)$ =ACCEPT
- For $x /\in L$, for any proof $\Pi \in \{0, 1\}$ poly(n) , $V (x, \Pi)$ = REJECT**[11]**

Definition 2. IP is a class of language L such that there is a randomized poly time verifier V such that

- For any $x \in L$, there exists a prover P such that Pr[V (x) = ACCEP T] = 1
- For $x /\in L$, for any prover P, Pr[V (x) = REJECT] ≥ 0.9 **[11]**

Definition 3. MIP is a class of language L such that there is a randomized poly time verifier V such that

- For any $x \in L$, there exists a proof $\Pi \in \{0, 1\}$ exp(n) such that Pr[V $\Pi(x)$ = ACCEP T] = 1 **[11]**
- For $x /\in L$, for all proof $\Pi \in \{0, 1\}$ exp(n) , Pr[V $\Pi(x)$ = REJECT] ≥ 0.9**[11]**

Definition 5. 3 SAT is a boolean formula φ in 3 CNF which is satisfiable. An example of 3 CNF : $(x1 \vee x2 \vee x\bar{\ }3) \wedge (\bar{\ }x1 \vee x4 \vee x7) \wedge (...)$ We know that 3 SAT is an NP complete problem. Similarly, we describe NEXP.**[11]**

Definition 6. SUCCINT-3CSP is a boolean formula $F : \{0, 1\} m \times \{0, 1\} 3l \times \{0, 1\} 3 \rightarrow \{0, 1\}$ which represents a function H on 2 l variables $x1, \cdots , x2 l$, $H(x1, \cdots , x2 l) = \wedge z \in \{0,1\}m,i,j,k \in \{0,1\}$ $lF(z, i, j, k, xi , xj , xk)$ such that H is satisfiable. (i.e., $\exists x1, \cdots , x2 l \in \{0, 1\}$ such that $H(x1, \cdots , x2 l) = 1$)**[11]**

Fact 7. SUCCINT-3CSP is NEXP complete. **[11]**

Definitions and proof: [11] [12][30][31]

NEEXP = ⊆ MIP*

The main result of this work is the inclusion NEEXP = NTIME[2^2^poly(n)] ⊆ MIP*. This is an exponential improvement over the prior lower bound and shows that proof systems with entangled provers are at least exponentially more powerful than classical provers. In our protocol the verifier delegates a classical, exponentially large MIP protocol for NEEXP to two entangled provers: the provers obtain their exponentially large questions by measuring their shared state, and use a classical PCP to certify the correctness of their exponentially-long answers. For the soundness of our protocol, it is crucial that each player should not only sample its own question correctly but also avoid performing measurements that would reveal the other player's sampled question. We ensure this by commanding the players to perform a complementary measurement, relying on the Heisenberg uncertainty principle to prevent the forbidden measurements from being performed.[32]

MIP* = RE

MIP*=RE shows that the class MIP* of languages that can be decided by a classical verifier interacting with multiple all-powerful quantum provers sharing entanglement is equal to the class RE of recursively enumerable languages. An immediate byproduct of this result is that there is an efficient reduction from the Halting Problem to the problem of deciding whether a two-player nonlocal game has entangled value 1 or at most 1/2. Using a known connection, undecidability of the entangled value implies a negative answer to Tsirelson's problem: MIP*=RE shows, by providing an explicit example, that the closure Cqa of the set of quantum tensor product correlations is strictly included in the set Cqc of quantum commuting correlations. Following work of (Fritz, Rev. Math. Phys. 2012) and (Junge et al., J. Math. Phys. 2011) this results provide a refutation of Connes' embedding conjecture from the theory of von Neumann algebras. **[0]**

III. Notes

Complexities

RE: (recursively enumerable) is the class of decision problems for which a 'yes' answer can be verified by a Turing machine in a finite amount of time [2]

NEXP:

-Nondeterministic exponential time (i.e. NTIME ($2^{p(n)}$) for p a polynomial)

-NEXP Equals MIP [BFL91] (but not relative to all oracles).

NEXP is in MIP* [IV12].

NEXP is in P/poly if and only if NEXP = MA [IKW01].

If P = RP, then NEXP is not computable by polynomial-size arithmetic circuits. [KI02]

NEXP Does not equal NP [SFM78].

NEXP Does not equal EXP if and only if there is a sparse set in NP that is not in P.

There exists an oracle relative to which EXP = NEXP but still P does not equal NP [Dek76].

The theory of reals with addition is hard for NEXP [FR74].

NEEXP:

Nondeterministic double-exponential time (i.e. NTIME($2^{2^{p(n)}}$) for p a polynomial). [4]

IP:

interactive Proof

Private coins may not be helpful, but more rounds of interaction are helpful. If we allow the probabilistic verifier machine and the all-powerful prover to interact for a polynomial number of rounds, we get the class of problems called **IP**. In 1992, Adi Shamir revealed in one of the central results of complexity theory that **IP** equals **PSPACE**, the class of problems solvable by an ordinary deterministic Turing machine in polynomial space.[]

MIP

One goal of **IP'**s designers was to create the most powerful possible interactive proof system, and at first it seems like it cannot be made more powerful without making the verifier more powerful and so impractical. Goldwasser et al. overcame this in their 1988 "Multi prover interactive proofs: How to remove intractability assumptions", which defines a variant of **IP** called **MIP** in which there are *two* independent provers.[14] The two provers cannot communicate once the verifier has begun sending messages to them. Just as it's easier to tell if a criminal is lying if he and his partner are interrogated in separate rooms, it's considerably easier to detect a malicious prover trying to trick the verifier into accepting a string not in the language if there is another prover it can double-check with.

In fact, this is so helpful that Babai, Fortnow, and Lund were able to show that **MIP** = **NEXPTIME**, the class of all problems solvable by a nondeterministic machine in *exponential time*, a very large class.[15] NEXPTIME contains PSPACE, and is believed to strictly contain PSPACE. Adding a constant number of additional provers beyond two does not enable recognition of any more languages. This result paved the way for the celebrated PCP theorem, which can be considered to be a "scaled-down" version of this theorem.[31]

MIP also has the helpful property that zero-knowledge proofs for every language in **NP** can be described without the assumption of one-way functions that **IP** must make. This has bearing on the design of provably unbreakable cryptographic algorithms.[14] Moreover, a **MIP** protocol can recognize all languages in **IP** in only a constant number of rounds, and if a third prover is added, it can recognize all languages in **NEXPTIME** in a constant number of rounds, showing again its power over **IP**.

It is known that for any constant *k*, a MIP system with *k* provers and polynomially many rounds can be turned into an equivalent system with only 2 provers, and a constant number of rounds.[16]

PCP (also referenced in quantum:

While the designers of IP considered generalizations of Babai's interactive proof systems, others considered restrictions. A very useful interactive proof system is PCP($f(n)$, $g(n)$), which is a restriction of MA where Arthur can only use $f(n)$ random bits and can only examine $g(n)$ bits of the proof certificate sent by Merlin.There are a number of easy-to-prove results about various PCP classes. The class of polynomial-time machines with no randomness but access to a certificate, is just NP. The class of polynomial-time machines with access to polynomially many random bits is co-RP.

Furthermore, the PCP theorem asserts that the number of proof accesses can be brought all the way down to a constant. They used this valuable characterization of NP to prove that approximation algorithms do not exist for the optimization versions of certain NP-complete problems unless P = NP. Such problems are now studied in the field known as hardness of approximation.[17][18]

MIP*: MIP* could be as large as RE, the class of recursively enumerable languages. (IE. MIP* = RE). MIP* is the class of languages which can be reliably verified by a classical, polynomial-time verifier interacting with multiple provers in different tensor factors of a Hilbert space. [0]

Connes' embedding conjecture

Connes' embedding problem, formulated by Alain Connes in the 1970s, is a major problem in von Neumann algebra theory. During that time, the problem was reformulated in several different areas of mathematics. Dan Voiculescu, developing his free entropy theory, found that Connes' embedding problem is related to the existence of microstates. Some results of von Neumann algebra theory can be obtained assuming a positive solution to the problem. The problem is connected to some basic questions in quantum theory, which led to the realization that it also has important implications in computer science.

The problem admits a number of equivalent formulations.[21] Notably, it is equivalent to the following long standing problems:

-Kirchberg's QWEP conjecture in C*-algebra theory

-Tsirelson's problem in quantum information theory

-The predual of any (separable) von Neumann algebra is finitely representable in the trace class.

In January 2020, Ji, Natarajan, Vidick, Wright, and Yuen announced a result in quantum complexity theory that implies a negative answer to Connes' embedding problem.[22][23][24][25][26][27][28][29]

Tsirelson's problem

Tsirelson's problem asks whether the set of nonlocal quantum correlations with a tensor product structure for the Hilbert space coincides with the one where only commutativity between observables located at different sites is assumed. Here it is shown that Kirchberg's QWEP conjecture on tensor products of C*-algebras would imply a positive answer to this question for all bipartite scenarios. This remains true also if one considers not only spatial correlations, but also spatiotemporal correlations, where each party is allowed to apply their measurements in temporal succession. [33]

von Neumann algebras

In mathematics, a von Neumann algebra or W*-algebra is a *-algebra of bounded operators on a Hilbert space that is closed in the weak operator topology and contains the identity operator. It is a special type of C*-algebra.

Von Neumann algebras were originally introduced by John von Neumann, motivated by his study of single operators, group representations, ergodic theory and quantum mechanics. His double commutant theorem shows that the analytic definition is equivalent to a purely algebraic definition as an algebra of symmetries.

There are three common ways to define von Neumann algebras.

The first and most common way is to define them as weakly closed *-algebras of bounded operators (on a Hilbert space) containing the identity. In this definition the weak (operator) topology can be replaced by many other common topologies including the strong, ultrastrong or ultraweak operator topologies. The *-algebras of bounded operators that are closed in the norm topology are C*-algebras, so in particular any von Neumann algebra is a C*-algebra.

The second definition is that a von Neumann algebra is a subset of the bounded operators closed under involution (the *-operation) and equal to its double commutant, or equivalently the commutant of some subset closed under *. The von

Neumann double commutant theorem (von Neumann 1930) says that the first two definitions are equivalent.

The first two definitions describe a von Neumann algebra concretely as a set of operators acting on some given Hilbert space. Sakai (1971) showed that von Neumann algebras can also be defined abstractly as C*-algebras that have a predual; in other words the von Neumann algebra, considered as a Banach space, is the dual of some other Banach space called the predual. The predual of a von Neumann algebra is in fact unique up to isomorphism. Some authors use "von Neumann algebra" for the algebras together with a Hilbert space action, and "W*-algebra" for the abstract concept, so a von Neumann algebra is a W*-algebra together with a Hilbert space and a suitable faithful unital action on the Hilbert space. The concrete and abstract definitions of a von Neumann algebra are similar to the concrete and abstract definitions of a C*-algebra, which can be defined either as norm-closed *-algebras of operators on a Hilbert space, or as Banach *-algebras such that $||aa^*||=||a||\ ||a^*||$.

Interactive proof systems

In computational complexity theory, an **interactive proof system** is an abstract machine that models computation as the exchange of messages between two parties: a *prover* and a *verifier*. The parties interact by exchanging messages in order to ascertain whether a given string belongs to a language or not. The prover possesses unlimited computational resources but cannot be trusted, while the verifier has bounded computation power but is assumed to be always honest. Messages are sent between the verifier and prover until the verifier has an answer to the problem and has "convinced" itself that it is correct.

All interactive proof systems have two requirements:

Completeness: if the statement is true, the honest verifier (that is, one following the protocol properly) can be convinced of this fact by an untrusted prover.

Soundness: if the statement is false, no prover, even if it doesn't follow the protocol, can convince the honest verifier that it is true, except with some small probability.

In a *public coin* protocol, the random choices made by the verifier are made public. They remain private in a private coin protocol.

Pauli basis measurements

Pauli matrices are named after the physicist Wolfgang Pauli. In quantum mechanics, they occur in the Pauli equation which takes into account the interaction of the spin of a particle with an external electromagnetic field.

Each Pauli matrix is Hermitian, and together with the identity matrix I (sometimes considered as the zeroth Pauli matrix σ_0), the Pauli matrices form a basis for the real vector space of 2 × 2 Hermitian matrices. This means that any 2 × 2 Hermitian matrix can be written in a unique way as a linear combination of Pauli matrices, with all coefficients being real numbers.

Time hierarchy theorem

In computational complexity theory, the time hierarchy theorems are important statements about time-bounded computation on Turing machines. Informally, these theorems say that given more time, a Turing machine can solve more problems. For example, there are problems that can be solved with n^2 time but not n time.

The time hierarchy theorem for deterministic multi-tape Turing machines was first proven by Richard E. Stearns and Juris Hartmanis in 1965.[17] It was improved a year later when F.C. Hennie and Richard E. Stearns improved the efficiency of the Universal Turing machine.[18] Consequent to the theorem, for every deterministic time-bounded complexity class, there is a strictly larger time-bounded complexity class, and so the time-bounded hierarchy of complexity classes does not completely collapse. More precisely, the time hierarchy theorem for deterministic Turing machines states that for all time-constructible functions $f(n)$,

quickly: the existence of an algorithm solving the task that runs in polynomial time, such that the time to complete the task varies as a polynomial function on the size of the input to the algorithm (as opposed to, say, exponential time).

IV. References

[0][22] Ji, Zhengfeng; Natarajan, Anand; Vidick, Thomas; Wright, John; Yuen, Henry (2020). "MIP*=RE". arXiv:2001.04383. Bibcode:2020arXiv200104383J.

[1]https://quantumfrontiers.com/2020/03/01/the-shape-of-mip-re/

[2]https://complexityzoo.net/Complexity_Zoo:R#re

[3]https://complexityzoo.net/Complexity_Zoo:N#nexp

[4]https://complexityzoo.net/Complexity_Zoo:N#ntime

[5]https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/nash-letters/nash_letters1.pdf

[6]https://ecommons.cornell.edu/bitstream/handle/ 1813/6910/89-994.pdf;jsessionid=DA253C639AFCC6A4DC159DC07702D403?sequence=1

[7] Shor, Mike. "Non-Cooperative Game". *GameTheory.net*. Retrieved 15 September 2016.

[8] Chandrasekaran, Ramaswamy. "Cooperative Game Theory"(PDF). University of Texas at Dallas.

[9] Brandenburger, Adam. "Cooperative Game Theory: Characteristic Functions, Allocations, Marginal Contribution"(PDF). Archived from the original (PDF) on 29 August 2017. Retrieved 14 April 2020.

[10] Owen, Guillermo (1995). *Game Theory: Third Edition*. Bingley: Emerald Group Publishing. p. 11. ISBN 978-0-12-531151-9.

[11]https://sites.math.rutgers.edu/~sk1233/courses/topics-S17/lec9.pdf

[12]https://people.cs.uchicago.edu/~fortnow/papers/mip2.pdf

[13] Adi Shamir. IP = PSPACE. *Journal of the ACM*, volume 39, issue 4, p.869–877. October 1992.

[14] M. Ben-or, Shafi Goldwasser, J. Kilian, and A. Wigderson. Multi prover interactive proofs: How to remove intractability assumptions. *Proceedings of the 20th ACM Symposium on Theory of Computing*, pp. 113–121. 1988.

[15] László Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, volume 1, pp. 3–40. 1991.

[16]http://groups.csail.mit.edu/cis/pubs/shafi/1988-stoc-bgkw.pdf

[17] Hartmanis, J.; Stearns, R. E. (1 May 1965). "On the computational complexity of algorithms". *Transactions of the American Mathematical Society*. American Mathematical Society. **117**: 285–306. doi:10.2307/1994208. ISSN 0002-9947. JSTOR 1994208. MR 0170805.

[18] Hennie, F. C.; Stearns, R. E. (October 1966). "Two-Tape Simulation of Multitape Turing Machines". *J. ACM*. New York, NY, USA: ACM. **13** (4): 533–546. doi:10.1145/321356.321362. ISSN 0004-5411.

[19] Goldwasser, S.; Micali, S.; Rackoff, C. (1989). "The knowledge complexity of interactive proof systems" (PDF). *SIAM Journal on Computing*. **18** (1): 186–208. doi:10.1137/0218012. ISSN 1095-7111. Extended abstract

[20] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. *Proceedings of ACM STOC'86*, pp. 58–68. 1986.

[21]Hadwin, Don (2001). "A Noncommutative Moment Problem". *Proceedings of the American Mathematical Society*. **129** (6): 1785–1791. doi:10.1090/S0002-9939-01-05772-0. JSTOR 2669132.

[23] Castelvecchi, Davide (2020). "How 'spooky' is quantum physics? The answer could be incalculable". *Nature*. **577** (7791): 461–462. Bibcode:2020Natur.577..461C. doi:10.1038/d41586-020-00120-6. PMID 31965099.

[24] Kalai, Gil (2020-01-17). "Amazing: Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen proved that MIP* = RE and thus disproved Connes 1976 Embedding Conjecture, and provided a negative answer to Tsirelson's problem". *Combinatorics and more*. Retrieved 2020-03-06.

[25] Barak, Boaz (2020-01-14). "MIP*=RE, disproving Connes embedding conjecture". *Windows On Theory*. Retrieved 2020-03-06.

[26] Aaronson, Scott (16 January 2020). "MIP*=RE". *Shtetl-Optimized*. Retrieved 2020-03-06.

[27] Regan, Kenneth W. (2020-01-15). "Halting Is Poly-Time Quantum Provable". *Gödel's Lost Letter and P=NP*. Retrieved 2020-03-06.

[28] Vidick, Thomas (2020-01-14). "A Masters project". *MyCQstate*. Retrieved 2020-03-06.

[29] Hartnett, Kevin (4 March 2020). "Landmark Computer Science Proof Cascades Through Physics and Math". *Quanta Magazine*. Retrieved 2020-03-09.

[30]http://www.cs.umd.edu/~jkatz/complexity/f11/lecture26-dapon.pdf

[31]https://people.cs.uchicago.edu/~fortnow/papers/mip2.pdf

[32] https://arxiv.org/pdf/1904.05870.pdf

[33]https://www.worldscientific.com/doi/abs/10.1142/S0129055X12500122

[IV12] T. Ito and T. Vidick. A multi-prover interactive proof for NEXP sound against entangled provers, to appear in *Proceedings of IEEE FOCS 2012* arXiv:1207.0550.

[BFL91] L. Babai, L. Fortnow, and C. Lund. Nondeterministic exponential time has two-prover interactive protocols, *Computational Complexity* 1:3-40, 1991. http://people.cs.uchicago.edu/~fortnow/papers/mip2.ps.

[Dek76] M. I. Dekhtyar. On the relativization of deterministic and nondeterministic complexity classes, *Mathematical Foundations of Computer Science*, pp. 255-259, Springer LNCS 45, 1976.

[IKW01] R. Impagliazzo, V. Kabanets, and A. Wigderson. In search of an easy witness: exponential time vs. probabilistic polynomial time, *Proceedings of IEEE Complexity'2001*, 2001.

http://www.cs.sfu.ca/~kabanets/papers/exp_journal.ps.gz

[KI02] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds, *Computational Complexity* 13:1–46, 2004. DOI:10.1007/s00037-004-0182-6, https://www.cs.sfu.ca/~kabanets/Research/poly.html

[SFM78] J. Seiferas, M. Fischer, and A. Meyer. Separating nondeterministic time complexity classes, *Journal of the ACM* 25:146-167, 1978.

[FR74] M. J. Fischer and M. O. Rabin. Super-exponential complexity of Presburger arithmetic, *Complexity of Computation* (R. M. Karp, ed.), SIAM-AMS Symposium on Applied Mathematics, 1974.