Multi-prover games and their parallel repetition

By

AMBO AMANDURE Jean-Médard (jeanmedard.ambo@aims.ac.rw)

June 2017

AN ESSAY PRESENTED TO AIMS RWANDA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE IN MATHEMATICAL SCIENCES

AIMS | African Institute for Mathematical Sciences
RWANDA

DECLARATION

This work was carried out at AIMS Rwanda in partial fulfilment of the requirements for a Master of Science Degree.

I hereby declare that except where due acknowledgement is made, this work has never been presented wholly or in part for the award of a degree at AIMS Rwanda or any other University.

Scan your signature

Student: Firstname Middlename Surname

Scan your signature

Supervisor: Firstname Middlename Surname

ACKNOWLEDGEMENTS

This is optional and should be at most half a page. Thanks Ma, Thanks Pa. One paragraph in normal language is the most respectful.

Do not use too much bold, any figures, or sign at the bottom.

DEDICATION

This is optional.

Abstract

A short, abstracted description of your essay goes here. It should be about 100 words long. But write it last.

An abstract is not a summary of your essay: it's an abstraction of that. It tells the readers why they should be interested in your essay but summarises all they need to know if they read no further.

The writing style used in an abstract is like the style used in the rest of your essay: concise, clear and direct. In the rest of the essay, however, you will introduce and use technical terms. In the abstract you should avoid them in order to make the result comprehensible to all.

You may like to repeat the abstract in your mother tongue.

Contents

1. Introduction

Games are inherent to human nature and are present in all cultures. In a game there are: goals, rules, challenges, interactions, conflicts, skill, strategies and chance (McGonigal, 2011; Crawford, 1984). History retains [Jan: s/retains/shows] that scientific study of the chance to win a game or of making decisions under uncertainty and risks has given birth to what we call nowadays probability theory which has a large application [Jan: s/a large application/many applications] (Freund, 2012). The mathematical study of rules of a game allows to compute the winning probability according to strategies used, and to determine the optimal strategy and the existence of a solution.

The game called *prover*, [Jan: s/the game called prover/the multi-prover games] introduced by Ben-Or, Goldwasser, Kilian, and Wigderson (1988) is a part [Jan: s/part/kind] of the games whose rules, strategies and outcomes have been mathematized. A prover game is a game which is played between at least two players called provers against a referee called also a verifier. A prover game is a concept originating from theoretical computer science.

Let us talk about what a prover game is.A prover game G is played between two provers 1 and 2 against the verifier ϕ. That is, the prover game is restricted to two players. Let X and Y be respectively the set of questions addressed to players 1 and 2. We denote by S and T respectively sets of answers to question set X and Y. The verifier samples a couple of questions $(x, y) \in_\mu Q \subseteq X \times Y$ according to the probability distribution μ on Q and sends the question x to the prover 1 and y to the prover 2. Their answers can be accepted or rejected by the verifier ϕ, that is the verifier is a predicate defined from $X \times Y \times S \times T$ to $\{0, 1\}$. Both provers win the game if the verifier accepts both answers, that is if $\phi(x, y, f(x), g(y)) = 1$ where f and g are strategies used respectively by the prover 1 and the prover 2. On the other hand, they lose. [Jan: s/On the other hand/Otherwise]. [Jan: Make clear that this is example for two provers.]

[Jan: I would include what you commented out here.]

Thus, the probability to win the game is the probability of the verifier to accept both answers. Therefore, the value of the game G denoted by $\mathrm{val}(G)$ is the winning probability of provers 1 and 2 when they use the optimal couple (f, g) of strategies, namely: $\mathrm{val}(G) = \max_{f,g} \Pr[\phi(x, y, f(x), g(y)) = 1]$.

Similarly, given such game G played between two provers 1 and 2 against a verifier. Let n be a natural number greater than 1. Based to the game G, [Jan: Based to/Based on] we can construct another game G^n called *$n-$fold parallel repetition of G* or *product game G^n*. In this game, the verifier samples independently n questions for each of the prover 1 and 2. He sends them all at once and receives n answers. The two provers win if the verifier accepts on all n instances, that is approximately speaking when n copies of the game G is tried to be won simultaneously. [Jan: Why "approximately speaking"? s/is tried to be won/are won] Thus, the value of the *$n-$fold parallel repetition of G* denoted by $\mathrm{val}(G^n)$ is the maximum success probability over all possible couple of strategies. Given $\mathrm{val}(G)$ for some non-trivial game, the determination of $\mathrm{val}(G^n)$ seems to be not simple. Raz (1998) gave an upper bound of $\mathrm{val}(G^n)$. This upper bound continues to be performed [Jan: s/performed/improved] (Holenstein, 2007; Raz and Rosen, 2012; Dinur and Steurer, 2014; Dinur et al., 2016).

The definition of two-prover games can be expanded similarly to multi-prover games, that is to a prover game with more than two players. However, a general result like Raz (1998) is not known for multi-prover games. [Jan: When you just say "prover game" it is not clear if it means two or multiple provers. I would say "two-prover" or "multi-prover" everywhere.]

Furthermore, mathematical games, namely games for which rules, strategies and outcomes have been mathematized are among applications of number theory, [Jan: s/among applications of/related to] especially of arithmetic combinatorics. [Jan: s/especially of/which in turn is related to] Verbitsky (1996) gave a general upper bound of the parallel repetition of two prover games by applying the density version of the Hales-Jewett theorem from the field called additive combinatorics. Tao and Vu (2006) define [Jan: s/define/describe] additive combinatorics as " *a marriage of number theory, harmonic analysis, combinatorics, and ideas from ergodic theory, which aims to understand very simple systems: the operations of addition and multiplication and how they interact*".

[Jan: Please mention more about additive combinatorics, at least VdW and Szemeredi's theorems.]

The density version of the Hales-Jewett theorem states that given natural number k, r, there exists a natural number $DHJ(k, r)$ such that every $n \geq DHJ(k, r)$ and every subset A of the set $\{1, 2, \ldots, k\}^n$ with density at least δ contains a combinatorial line (Polymath, 2012).

Thus, the aim of this research is to analyse the relationship between the Hales-Jewett theorem and the parallel repetition of multi-prover games. Specifically, first this study explores what the Hales-Jewett theorem is and what parallel repetition of multi-prover games is. Then, the study generalizes some notions defined for two-prover games to multi-prover games. Finally, this study shows that Hales-Jewett theorem implies parallel repetition and also parallel repetition implies the Hales-Jewett theorem.

Parallel repetition of prover games finds its application in many areas: hardness of approximation, cryptography, quantum mechanics, interactive proof systems, probabilistically checkable proofs Tamaki (2015); Dinur et al. (2016). That is, a main application of prover games is in proving that certain computational problems are difficult not only to solve exactly but also to approximate.

(Ben-Or et al., 1990) presented a concrete application in real life of what can mean two provers and the verifier. He considered that the verifier is the Bank, which interacts with two untrusted provers, for instance two bank identification cards. The two provers can jointly agree on a strategy to convince the verifier of their identity. However, to believe the validity of their identity proving procedure, the verifier must make sure that the two provers can not communicate with each other during the course of the proof process.

[Jan: The last two paragraphs should be put earlier (when you describe games).]

By establishing the connection between parallel repetition of multi-prover games and the density version of the Hales-Jewett theorem, we want to show that we can always find a result that connects disparate fields of mathematics.

This research is composed of four chapters where the introduction is the first chapter. In chapter 2, an exploration on the Hales-Jewett theorem is presented. These implications are shown: Hales-Jewett theorem implies Van der Waerden's theorem, Hales-Jewett theorem implies Szemerédi's theorem and Szemerédi's theorem implies Van der Waerden's theorem. Chapter 3 deals with the parallel repetition of multi-prover games. Also, a generalisation of known notions on two-prover games is presented. Chapter 4 analyses the relationship between parallel repetition of multi-prover games and the Hales-Jewett theorem.

2. On the Hales-Jewett theorem

In this part, some notions about Hales-Jewett theorem are presented. Firstly, we start by some basic notions on arithmetic progression, which are important for understanding the next point. After, we introduce some elementary notions about Van der Waerden's theorem and Szemerédi's theorem. We highlight that Van der Waerden's theorem is a particular case of Szemerédi's theorem. Ultimately, we present the two forms of Hales-Jewett theorem and link these one to the two first theorems.

2.1 Arithmetic progression

2.1.1 Definition. Let $a_1, a_2, \ldots, a_n, \ldots$ be a sequence of numbers.

This sequence of numbers form an **arithmetic sequence** if every term of this sequence is obtained by adding a constant to the previous term.

The constant is simply the difference between two consecutive terms.

If a_1 and a_n represent the first and the $n-$th term of a sequence, and d the constant, then the general term a_n of this sequence is expressed as:

$$a_n = a_1 + (n-1)d.$$

Knowing a_m and the constant d, then a_n can be expressed as:

$$a_n = a_m + (n-m)d.$$

2.1.2 Arithmetic progression of length k. Let a and d be two fixed numbers.

An arithmetic progression of length k is an arithmetic progression of k numbers of the form $a+nd$. a is the first term of the arithmetic progression, d is the difference between two consecutive terms and $n = 0, 1, \ldots, k-1$, that is k consecutive values of n.

We denote by AP(k) or AP$-k$ or $k-$AP, the arithmetic progression of length k.

2.2 Van der Waerden's theorem

Before stating the Van der Waerden's theorem, let us introduce and define some concepts and notation.

A *partition* of a set A is a collection of nonempty and mutually disjoint subsets A_i of A, such that $A = \cup A_i$ and $A_i \cap A_j = \emptyset, \quad i \neq j$. Thus, a partition is also a sequence $A_1, A_2, \ldots, A_n$ of mutually nonempty and disjoint subsets of set A. A_i are known as *blocks*.

We denote by $\mathbb{Z}^+$, the set of positive integers. Let $m \in Z^+$, we designate by $[m]$ the set $\{1, 2, \dots, m\}$.

Let X be a set and r be a positive integer. We want to colour elements of set X with r colours. If C represents the set of colours, then $|C| = r$ is the number of colours.

2.2.1 Definition. An $r-$colouring of X is a mapping $c : X \longrightarrow [r]$.

[Jan: Still a problem here: You should write r-coloring, with - outside math mode.]

If $|X| = n$, then the number of r-colorings of X is n^r.

Let Y be a subset of X. Y is *monochromatic* when the restriction $c \restriction_Y$ is constant, that is if $c(y)$ is the same for every $y \in Y$.

According to Polymath (2012), the Van der Waerden's theorem is stated as follows:

2.2.2 Theorem (Van der Waerden). *For every pair $(k, r) \in \mathbb{Z}^+ \times \mathbb{Z}^+$, there exists $N_0 \in \mathbb{Z}^+$ such that for every $N \geq N_0$ and for every $r-$colouring of $[N]$ there is a monochromatic arithmetic progression of length k.*

We know that an $r-$colouring is a function called c in definition (2.2.1). So, in other words we can find at least one subset of $\{1, 2, \dots, N\}$ with $k-$elements such that all elements have the same colour and form an arithmetic progression of length k. That is, there exit [Jan: s/exit/exist] $a,\ d\ \in \mathbb{N}$ with $d \neq 0$ such that: $c(a) = c(a + d) = c(a + 2d) = \dots = c(a + (k - 1)d)$ where $a, a + 2d, \dots, a + (k - 1)d$ are elements of the subset.

This Van der Waerden's theorem can also be formulated using partition (Dransfield et al., 2004) as:

2.2.3 Theorem (Van der Waerden). *For every $k, r \in \mathbb{Z}^+$, there exists $N_0 \in \mathbb{Z}^+$ such that for every $N \geq N_0$ and for every partition $A_1, \dots, A_r$ of $[N]$, there is i, $1 \leq i \leq r$, such that the block A_i contains an arithmetic progression of length k.*

Note that for this version a block in a partition can be empty.

The existence of the number N_0 for which any $r-$colouring of the integer $\{1, \dots, N_0\}$ is certain to have a monochromatic subset of cardinality k of which elements form an arithmetic progression was demonstrated constructively in 1927 by Bartel Leendert van der Waerden in Van der Waerden (1927).

Graham and Rothschild (1974) gave *another* proof of this theorem. The book entitled "*Purely Combinatorial Proofs of Van Der Waerden-Type Theorem*" written by Gasarch et al. (2010) condenses the proof of Van Der Waerden theorem. [Jan: Be careful with capitalization: it is "Van der Waerden's theorem".]

In this theorem, the difficult problem is to find the number N. [Jan: Rephrase this. Even showing that N_0 is not trivial (also correct typo $N- > N_0$).] The least such number N_0 is called *Van der Waerden number* denoted as $W(k, r)$. In the rest of this chapter, we will use $W(k, r)$ or simply W to denote the least Van der Waerden number instead of N_0.

The general expression of $W(k, r)$ is not known, but for some k and r there are exact values known or there are some approximations of the lower or upper bound of $W(k, r)$ (Dransfield et al., 2004).

$W(1, r)$, $W(k, 1)$ and $W(2, r)$ are known as *trivial* Van der Waerden numbers. So,

- $W(1, r) = 1$: the set of all subsets of a nonempty set contains necessary a singleton. A singleton forms an arithmetic progression of length 1 where the difference between two consecutive numbers is 0. To form a monochromatic arithmetic progression of length 1 by $r-$colouring a set, we need a set of at least one element.
- $W(k, 1) = k$: by colouring a set with one colour, we automatically get a monochromatic arithmetic progression of length equals to the cardinality of the set.
- $W(2, r) = r + 1$: to obtain a monochromatic arithmetic progression of length 2 by $r-$colouring a set, we need a set of at least $r + 1$ elements.

For instance, let us find the Van der Waerden number $W(3, 2)$, that is a $2-$colouring of the set $[W(3, 2)]$ such that there is a monochromatic arithmetic progression of length 3. [Jan: Rephrase: ...that is N_0 such that every 2-coloring of $[N_0]$ contains a monochromatic...]

The value of $W(3, 2)$ is greater than 8 because for any $2-$colouring of $[n]$, $n \in \{3, 4, 5, 6, 7, 8\}$, we can find a $2-$colouring which does not contain a monochromatic arithmetic progression of length 3. For instance, the set $\{1, 2, \ldots, 8\}$ doest not contain a monochromatic arithmetic progression of length 3 by $2-$colouring the set like in the table (2.1).

So, when $W(3, 2) = 9$ we always find a monochromatic arithmetic progression of length 3 for any $2-$colouring of $[9]$. The table (2.1) shows one of the possibilities of colouring $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. If the ninth number is blue, then 3, 6, 9 form an arithmetic progression. If the ninth number is red, then 1, 5, 9 form an arithmetic progression. Therefore, by adding a ninth number and colouring it using any of the two colors, we always create a monochromatic arithmetic progression of length 3.

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

Table 2.1: A $2-$colouring of $\{1, 2, \ldots, 9\}$

[Jan: This example is now very well explained!]

The table (2.2) presents the 7 exact non-trivial Van der numbers (when $k \geq 3$) (Dransfield et al., 2004).

As related previously, searching for the exact value of $W(k, r)$ remains a difficult problem. [Jan: s/difficult/open and then delete next sentence.] By the way, it is an open problem. The number $W(k, r)$ becomes hard to find when the values of k and r increase. However, for some k and r there is an approximation of the lower or upper bound of $W(k, r)$ (Stevens and Shantaram,

$k \setminus r$	2	3	4
3	9	27	76
4	35	293	
5	178		
6	1132		

Table 2.2: The 7 exact non-trivial values of Van der Waerden numbers.

1978; Herwig et al., 2007; Beeler and O'neil, 1979; Dransfield et al., 2004; Brown et al., 2008; Rabung and Lotts, 2012; Kouril and Paul, 2008). The table (2.3) summarizes these known lower bounds and includes the seven non-trivial Van der Waerden numbers known exactly.

k \ r	**2**	**3**	**4**	**5**	**6**
3	9	27	76	>170	>223
4	35	293	>1,048	>2,254	>9,778
5	178	>2,173	>17,705	>98,740	>98,748
6	1,132	>11,191	>91,331	>540,025	>816,981
7	>3,703	>48,811	>420,217	>1,381,687	>7,465,909
8	>11,495	>238,400	>2,388,317	>10,743,258	>57,445,718
9	>41,265	>932,745	>10,898,729	>79,706,009	>458,062,329
10	>103,474	>4,173,724	>76,049,218	>542,694,970	>2,615,305,384
11	>193,941	>18,603,731	>305,513,57	>2,967,283,511	>3,004,668,671

Table 2.3: Some lower bounds and exact non-trivial values of Van der Waerden numbers $W(k, r)$.

The estimation of lower and upper bounds is also an open problem. There exist some expressions that bound Van der Waerden numbers. Researchers are still looking for closer bound or exact general expression of these numbers. Erdos and Rado (1952), cited by Dransfield et al. (2004) established an inequality for the lower bound for $W(k, r)$.

$$\left[2(k-1)r^{k-1}\right]^{\frac{1}{2}} < W(k, r). \tag{2.2.1}$$

Berlekamp (1968) found a better bound when $k-1$ is prime number and for $r = 2$. But these bounds still require improvement.

$$(k-1)2^{k-1} < W(k, 2). \tag{2.2.2}$$

For $p = k - 1$, the expression (2.2.2) becomes:

$$p2^p < W(p+1, 2). \tag{2.2.3}$$

So, $W(6, 2) > 5 \times 2^5 = 160$, $W(8, 2) > 7 \times 2^7 = 896$ and $W(12, 2) > 11 \times 2^11 = 22528$. (Dransfield et al., 2004) improve this lower bound by using propositional satisfiability solvers for some small van der Waerden numbers for instance $W(8,2) > 1322$. Rabung and Lotts (2012) performs more. Thus, as related in table (2.3), most of the lower bounds used came from Rabung and Lotts (2012).

The best known upper bound of $W(k,r)$ is the expression (2.2.4) which came from the work of Gowers (2001) on a new proof of Szemerédi's theorem. Section (2.3) will talk about this theorem. Szemerédi's theorem is the extension of Van der Waerden's theorem, that is Van der Waerden's theorem is a particular case of Szemerédi's theorem: [Jan: s/is a particular case/is implied by]

$$W(k,r) \leq 2^{2^{r^{2^{2^{k+9}}}}} \tag{2.2.4}$$

[Jan: This section is well written, good job.]

2.3 Szemerédi's theorem

Szemerédi's theorem is merely another formulation of Van der Waerden's theorem in terms of *density version*. Below, we show that Szemerédi's theorem implies Van der Waerden's theorem.

Let us consider A a nonempty subset of the set $[N]$. The density of A inside $[N]$ is a positive real number $\delta = \frac{|A|}{N}$. It is clear that $0 < \delta \leq 1$.

The theorem (2.3.1) is the famous Szemerédi's theorem. Famous because the various proofs of Szemerédi's theorem connect disparate fields of mathematics (combinatorics, harmonic analysis, ergodic theory, number theory, ...). Arana (2015) analysed the depth of Szemerédi's theorem by assembling the thoughts of some mathematicians (like Erdos and Terence Tao) about the major accomplishment of this theorem.

2.3.1 Theorem (Polymath (2012)). *For every $k \in \mathbb{Z}^+$ and every $0 < \delta \leq 1$ there exists an integer $N_0(k,\delta) \geq 1$ such that for every $N \geq N_0$ and every subset $A \subseteq [N]$ of size $|A| \geq \delta N$ contains an arithmetic progression of length k.*

[Jan: Don't cite Polymath above. This is still not fixed. You can say something like "according to polymath2012new".]

The Szemerédi's theorem has a formulation which uses the notion of positive upper density. Let A be a subset of the integers $\mathbb{Z}$ with positive upper density, that is, satisfying $\lim\sup_{N\to\infty} \frac{|A\cap[-N,N]|}{|[-N,N]|} > 0$. [Jan: Put the formula on separate line.] Then for any $k \geq 3$, A contains infinitely many arithmetic progressions of length k.

As conjecture, Szemerédi's theorem was formulated by Erdös and Turán (1936). There are several proofs of this theorem. The cases $k = 1$ and $k = 2$ are trivial. Roth (1953, 1970) proved the case $k = 3$. The case $k = 4$ was proved by Szemerédi (1969) and he gave the general case (Szemerédi, 1975).

Some of proofs necessitated the use of other theories external to combinatoric. Thus, the ergodic theory (*theory related to dynamical system with invariant measures and chaos theory*) has been used to prove this theorem by Furstenberg (1977); Furstenberg et al. (1982). [Jan: Use \cite* to avoid et al.] Gowers (1998, 2001) used Fourier analysis and the inverse theory of additive combinatorics. Gowers (2007) used a hypergraph regularity lemma to prove this theorem. A quantitative ergodic theory proof, version of Furstenberg et al. (1982) has been presented by Tao (2006) which does not involve some concepts used in the previous proofs: the axiom of choice, the use of infinite sets or measures, the use of the Fourier transform or inverse theorems from additive combinatorics.

2.3.2 Szemerédi's theorem implies Van der Waerden's theorem..

Proof. Let us assume that Szemerédi's theorem (2.3.1) is true, that is $\forall k \in \mathbb{Z}^+$, $0 < \delta \leq 1$, $\exists N_0(k,\delta) \in \mathbb{Z}^+ / \forall N \geq N_0$ and $\forall A \subseteq [N]$, $|A| \geq \delta N$ contains an arithmetic progression of length k. So, the aim is to show Van der Waerden's theorem from Szemerédi's theorem. This means to show that by $r-$colouring the set $\{1, 2, \ldots, N\}$, we obtain at least one monochromatic arithmetic progression of length k.

Let us notice that we have shown (2.2.2) and (2.2.3) that $r-$colouring a set is to partition it to r blocks.

Let $A_1, A_2, \ldots, A_r$ be a partition of $\{1, \ldots, N\}$ in r blocks, that is $\{1, \ldots, N\} = A_1 \cup A_2 \cup \ldots \cup A_r$, with $A_i \cap A_j \neq 0$ for two nonempty sets. [Jan: Correct typo in formula. Also empty blocks is not a problem.] But, sometimes a block can be empty. For instance, when $r > N$, that is the number of colors is bigger than the number of elements of the set to colour.

When $r < N$, there exist two blocks with the same colour. [Jan: Delete previous sentence. Think about case with empty blocks to see there are no problems with them.] Note that the color of the block A_i is indicated by the number i for $1 \leq i \leq r$.

Let A_{max} be the set having the largest number of elements. By partitioning $\{1, \ldots, N\}$ to r equal parts, we have: $A_{max} = A_i = \frac{N}{r}$, [Jan: Make clear that last sentence is just an example.]

Let us show that the cardinality of all A_i for $1 \leq i \leq r$ can not be less that $\frac{N}{r}$. [Jan: Rephrase: ... it cannot be that the cardinality of every A_i is less than...] Let us assume that $|A_i| < \frac{N}{r}$, then $|A_1| + |A_2| + \ldots + |A_r| < \frac{N}{r} + \ldots + \frac{N}{r} = \frac{rN}{r} = N$, that is $\displaystyle\sum_{i=1}^{r} |A_i| < N$. Therefore, for $1 \leq i \leq r$, in this case A_i does not form a partition which is a contradiction.

Hence,the cardinality of some of A_i is greater or equal to $\frac{N}{r}$. Obviously, the cardinality of A_{max} is greater or equal to the cardinality of A_i, that is $|A_{max}| \geq |A_i|$, for $1 \leq i \leq r$.

So, [Jan: First step below is not equivalence (just $\Longrightarrow$). Also, consider deleting step 3.]

$$\begin{aligned}|A_1| + |A_2| + \ldots + |A_r| = N &\iff |A_{max}| + |A_{max}| + \ldots + |A_{max}| \geq N \\ &\iff r|A_{max}| \geq N \\ &\iff |A_{max}| \geq \frac{N}{r} \\ &\iff |A_{max}| \geq \frac{1}{r}N \\ &\iff |A_{max}| \geq \delta N\end{aligned}$$

where $\delta = \frac{1}{r}$. As $|A_{max}| \geq \delta N$ and according to Szemerédi's theorem (2.3.1) the subset A_{max} contains an arithmetic progression of length k. [Jan: For $N \geq N_0(k, 1/r)$. You have to say this!] Note that A_{max} is monochromatic because it has been obtained by $r-$colouring the set $\{1, 2, \ldots, N\}$.

Therefore, A_{max} is a monochromatic arithmetic progression of length k. [Jan: A_{max} contains a progression.] □

This proof show that we can obtain Van der Waerden's theorem from Szemerédi's theorem when $\delta = \frac{1}{r}$.

2.3.3 Quantitative bounds of Szemerédi's theorem. In the previous section (2.3.2) we have shown that Van der Waerden's theorem is a particular case of Szemerédi's theorem. This implies that the Szemerédi's number $N(k, \delta)$ is less or equal to the Van der Waerden's number $W(k, r)$ when $\delta = \frac{1}{r}$. [Jan: greater than or equal] There is still no general exact expression of $W(k, r)$, but we have shown previously that only the exact value of 7 non-trivial Van der Waerden numbers are known for some smaller k and r. For the remain cases there are only some approximations of the lower and upper bounds.

As for Van der Waerden's numbers, the general expression of Szemerédi's numbers $N(k, \delta)$ is not known. The search for this number is an open problem. However, there are some quantitative approximations of the lower and upper bounds of the Szemerédi's numbers. The following definition will be helpful for the approximation of the lower and upper bounds of Szemerédi's numbers $N(k, \delta)$.

2.3.4 Definition. Let $N = N(k, \delta)$ be the Szemerédi's number such that all subsets of the integers $\{1, 2, \ldots, N\}$ with positive upper density contain arbitrarily long arithmetic progressions. [Jan: I don't get the purpose of this sentence. Also it is not correct.]

Let V be the largest subset of $\{1, 2, \ldots, N\}$ without an arithmetic progression of length k.

We denote by $r_{k,N}$ the size of the set $V : \delta_{k,N} = |V|$.

The *density of* V denoted by $\delta_{k,N}$ is defined as:

$$\delta_{k,N} = \frac{|V|}{N}$$

In the following expressions for the estimation of lower and upper bounds of $\delta_{k,N}$, the logarithms used are binary.

Lower bound Behrend (1946) constructed the lower bound of the density of the largest subset of $\{1, 2, \ldots, N\}$ that contains no arithmetic progression of length $k = 3$. He proved that for any $\epsilon > 0$ and for an unspecified positive constant :

$$\delta_{3,N} \geq \frac{C}{2^{2\sqrt{2}(1+\epsilon)\sqrt{\log N}}} \tag{2.3.1}$$

Elkin (2010) improved the result of Behrend (2.3.1) by a factor $\Theta(\sqrt{\log N})$[1] and showed that:

$$\delta_{3,N} \geq \frac{C(\log N)^{1/4}}{2^{2\sqrt{2}\sqrt{\log N}}} \tag{2.3.2}$$

[Jan: $\sqrt{\log N}$ or $(\log N)^{1/4}$? THis is still not fixed.]

For $k \geq 1 + 2^{n-1}$, $n = \lceil \log k \rceil$, Robert Alexander Rankin in 1961, cited by O'Bryant (2011) proved that for $\epsilon > 0$, if N is sufficiently large then:

$$\delta_{k,N} \geq \frac{C}{2^{n2^{(n-1)/2}(1+\epsilon)\sqrt[n]{\log N}}} \tag{2.3.3}$$

Basing on (2.3.1), (2.3.2) and (2.3.3), O'Bryant (2011) constructed a general lower bound (2.3.4) for the density of the largest subset of $\{1, 2, \ldots, N\}$ that contains no arithmetic progression of length k.

$$\delta_{k,N} \geq C_k 2^{-n2^{(n-1)/2}\sqrt[n]{\log N}+\frac{1}{2n}\log\log N} \tag{2.3.4}$$

where $C_k > 0$ is an unspecified constant. The expression (2.3.4) is presently the best known lower bounds for all k.

Upper bound Gowers (2001) worked on a new proof of Szemerédi's theorem and presented that the upper bound of the density of the largest subset of $\{1, 2, \ldots, N\}$ that contains no arithmetic progression of length k is:

$$\delta_{k,N} \leq (\log\log N)^{-2^{-2^{k+9}}} \tag{2.3.5}$$

Bloom (2016) improved the upper bound for $k = 3$:

$$\delta_{3,N} \leq C\frac{(\log\log N)^4}{\log N}. \tag{2.3.6}$$

For $k = 4$, Green and Tao (2006) improved the result (2.3.5) of Gowers (2001) as follows:

$$\delta_{4,N} \leq CNe^{-c\sqrt{\log\log N}} \tag{2.3.7}$$

for some absolute constant $c > 0$.

Therefore, by combining the lower (2.3.4) and upper (2.3.5) bounds of $\delta_{k,N}$ we have:

$$C_k 2^{-n2^{(n-1)/2}\sqrt[n]{\log N}+\frac{1}{2n}\log\log N} \leq \delta_{k,N} \leq (\log\log N)^{-2^{-2^{k+9}}} \tag{2.3.8}$$

[Jan: The section on the bounds is still too many formulas, too little explanations. For the last equation I suggest you write best known formulas for $k = 3$ for easier comparison.]

[1] The big Theta (Θ) expresses the tight asymptotic bounds, that is the intersection of the upper asymptotic bounds (big-O) and the lower asymptotic bounds (big-Ω)

2.4 Hales-Jewett theorem

[Jan: Make section title: Hales-Jewett theorem and its density version.]

Before stating the Hales-Jewett theorem, let us introduce and define notions about combinatorial lines. Combinatorial line is for Hales-Jewett theorem what arithmetic progression is for Van der Waerden's theorem, that is Hales-Jewett theorem is based on structures called combinatorial lines.

Let k and n be two positive integers.

We know that $[k]^n = \underbrace{[k] \times [k] \times \ldots \times [k]}_{n \text{ set-factors of } [k]} = \{(x_1, x_2, \ldots, x_n) : \ x_i \in [k]\}$. The set $[k]^n$ contains k^n elements.

For instance, for $k = 3$ and $n = 2$, $[3]^2 = \{11, 12, 13, 21, 22, 23, 31, 32, 33\}$. For $k = 3$ and $n = 6$, an element of the set $[3]^6$ is : 121132. In total, in the set $[3]^6$ there are 729 different elements.

Let us consider the set $([k] \times \{x\})^n$. Similarly, the set $([k] \times \{x\})^n$ contains $(k+1)^n$ elements. x is called *wildcard*.

Given $k, n \in \mathbb{N}$, we call $x-$*string* (or $n-$dimensional *variable word* with k letters or alphabets), a finite word $a_1 a_2 \ldots a_n$ of the symboles [Jan: s/symboles/symbols] $a_i \in [k] \cup \{x\}$, where at least one symbol a_i is x. We denote an $x-$string by $w(x)$. Let D denote the set of all strings: $D = \{w(x)\}$. The cardinality of D is: $D = (k+1)^n - k^n$.

For any integer $i \in [k]$ and $x-$string $w(x)$, we denote by $w(x; i)$ the string obtained from $w(x)$ by replacing each x by i.

2.4.1 Definition. A *combinatorial line* is a set of k strings $\{w(x; i) : \ i \in [k]\}$ where $w(x)$ is an $x - string$.

[Jan: Too much in math mode for x-string.]

That is a combinatorial line is a set of k finite words obtained by replacing x in the word $w(x; i)$ by $i \in \{1, 2, \ldots k\}$. A combinatorial line can also be written as a $k \times n$ matrix in this case, where columns are composed either by $(a_i a_i \ldots a_i)^T$ or by $(12\ldots)^T$ (T denotes transpose).

For instance, the number of combinatorial lines in $[3]^2 = \{11, 12, 13, 21, 22, 23, 31, 32, 33\}$ is $(3+1)^2 - 3^2 = 16 - 9 = 7$. These 7 combinatorial lines are given in figure (2.1) which correspond each to the winning position of a tic-tac-toe game. The diagonal winning position $\{13, 22, 31\}$ in a tic-tac-toe is not a combinatorial line.

For $k = 3$ and $n = 8$, a combinatorial line over alphabets $\{1, 2, 3\}$ for the word $w(x) = 1xx2x23x$ is the set :

$\{w(x; i) = 1ii2i23i : \ i \in [3]\} = \{11121231, 12222232, 13323233\}$. As matrix representation, this combinatorial line can be expressed as:

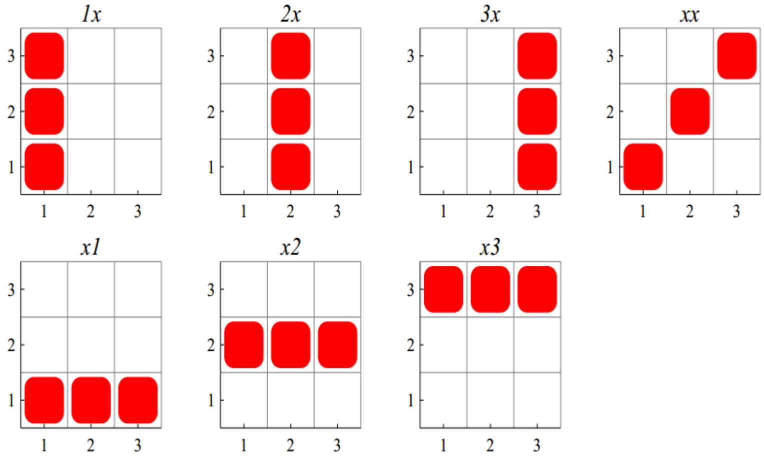

Figure 2.1: Combinatorial lines in $[3]^2$ (Source: Polymath (2010))

$$\begin{pmatrix} 1 & 1 & 1 & 2 & 1 & 2 & 3 & 1 \\ 1 & 2 & 2 & 2 & 2 & 2 & 3 & 2 \\ 1 & 3 & 3 & 2 & 3 & 2 & 3 & 3 \end{pmatrix}$$

Sets which do not contain any combinatorial lines are called *line-free*.

2.4.2 Theorem (Hales-Jewett theorem). *For every pair of positive integers k and r there exists a positive number $HJ(k,r)$ such that for every $n \geq HJ(k,r)$ and every $r-$colouring of the set $[k]^n$ there is a monochromatic combinatorial line.*

There are several proofs of Hales-Jewett theorem. The original proof has been given by Hales and Jewett (1987). Shelah (1988) proved a primitive recursive[2] bound for the Hales-Jewett number using simple induction. Nilli (1990) presented a compact form of Shelah's Proof of the Hales-Jewett Theorem. This condensed form states that for every $k, r \geq 1$, $HJ(k,r) \leq \frac{1}{kr} h_4(k+m+2)$ where the function h_i is defined as: $h_1(n) = 2n$; for $i > 1$, $h_i = \underbrace{h_{i-1}(h_{i-1}(\dots h_{i-1}(1)))}_{h_{i-1} \text{ is taken } n \text{ times}}$. [Jan: s/$h_i$/$h_i(n)$. Also put this formula as separate equation.] !

Matet (2007) gave a variant of Shelah's proof of the Hales–Jewett theorem by replacing Shelah's pigeonhole lemma by an appeal to Ramsey's theorem.

The Hales-Jewett theorem has also a density version. By considering a nonempty subset A of the set $[k]^n$, the density of A inside $[k]^n$ is a positive real number $\delta = \frac{|A|}{k^n}$. Values of δ are bounded by 0 and 1, that is $0 < \delta \leq 1$.

Let denote by $DHJ(k,\delta)$ the density Hales-Jewett number. The density version of Hales-Jewett theorem is announced as follows:

[2] Primitive recursion is a procedure that defines the value of a function at an argument n by using its value at the previous argument $n-1$. On computer, a primitive recursive bound can be implemented only using do-loops (see https://plato.stanford.edu/entries/recursive-functions/#1.3).

2.4.3 Theorem (Density version of Hales-Jewett theorem). *For any $k \in \mathbb{Z}^+$ and any real number $0 < \delta \leq 1$, there exists a positive integer $DHJ(k, \delta)$ such that if $n \geq DHJ(k, \delta)$ and A is any subset of $[k]^n$ with $|A| \geq \delta k^n$, then A contains a combinatorial line.*

The proof of the density version of Hales-Jewett theorem has been demonstrated by Furstenberg and Katznelson (1991) using ergodic methods[3]. Polymath (2012) gave an elementary non-ergodic proof of the density version of Hales-Jewett theorem by giving a quantitative bound on how large n needs to be and qualified this theorem as one of the fundamental results of Ramsey theorey. A simplified version of Polymath (2012) has been given by Dodos et al. (2013) using a purely combinatorial proof of the density Hales–Jewett Theorem.

There are four important theorems we have talked about: Van der Waerden's theorem (2.2.2), Szemerédi's theorem (2.3.1), Hales-Jewett theorem (2.4.2) and density Hales-Jewett theorem (2.4.3). In (2.3.2) we have shown that Szemeredi's theorem implies Van der Waerden's theorem. It is reasonable to show these three implications: the density version of Hales-Jewett theorem implies the Hales-Jewett theorem [Jan: Put comma here.] Hales-Jewett theorem implies Van der Waerden's theorem, and the density version of Hales-Jewett theorem implies Szemerédi's theorem.

2.4.4 Density version of Hales-Jewett theorem implies the Hales-Jewett theorem. To show that this density version of Hales-Jewett theorem implies the Hales-Jewett theorem, we need only to set as in (2.3.2), $\delta = \frac{1}{r}$. By $r-$colouring the set $[k]^n$, that is by partitioning to r classes, if A_{max} is the set containing the maximum number then $|A_{max}| \geq \frac{k^n}{r} = \delta k^n$. Hence, according to (2.4.3), A_{max} contains a combinatorial line.

2.4.5 Hales-Jewett theorem implies Van der Waerden's theorem. To show that the Hales-Jewett theorem implies Van der Waerden's theorem, we need only to show that combinatorial line corresponds to the arithmetic progression.

Let us assume that the Hales-Jewett theorem is true and show that the combinatorial line of k elements contained to the subset A corresponds to the arithmetic progression of length k.

We have defined $[k]$ as the set $\{1, 2, \ldots, k\}$. Instead to start by 1, let us start by 0. In this part, $[k]$ expresses the set $\{0, 1, \ldots, k-1\}$. It is obvious that $[k] = \mathbb{Z}/k\mathbb{Z}$.

Let n be the positive number of the Hales-Jewett theorem, then the set $[k]^n = (\mathbb{Z}/k\mathbb{Z})^n = \{(y_0, y_1, \ldots, y_{n-1}) : \ y_i \in [k]\}$ has k^n elements. Similarly, $[k^n] = \{0, 1, \ldots, k^n - 1\}$ has also k^n elements. Note that the set $[k^n]$ contains natural number (in base 10). [Jan: Just natural numbers, not in any base.] While, elements of the set $[k]^n$ are [Jan: s/are/can be interpreted as] the digits in base$-k$ number system of the numbers $\{0, 1, \ldots, k^n - 1\}$.

Let us consider the bijection $f : [k]^n \longrightarrow [k^n]$ defines as follows:

$$f(y_0, y_1, \ldots, y_{n-1}) = y_0 + y_1 k + y_2 k^2 + \ldots + y_{n-1} k^{n-1}.$$

[3] Ergodic theory studies dynamical systems with an invariant measure and related problems. Ergodic theory can be described as the statistical and qualitative behavior of measurable group and semigroup actions on measure spaces.

Let $w(x) \in ([k] \cup \{x\})^n \setminus [k]^n$ be an $x-tring$. The combinatorial line generates by $w(x)$ is a set of k elements defined by $\{w(x;i) : i \in [k]\}$.

Let $w(x;i)$ and $w(x;i+1)$ be two consecutive elements of the combinatorial line generates by $w(x)$. We denote $w(x;i) = (y_{0,i}, y_{1,i}, \ldots, y_{n-1,i})$ and $w(x;i+1) = (y_{0,i+1}, y_{1,i+1}, \ldots, y_{n-1,i+1})$ where the elements $y_{j,i} \in [k]$ for $0 \leq j \leq n-1$ and $0 \leq i \leq k-1$.

The difference [Jan: Mention that your arithmetics now is in a vector space (so $w(x;i)$ is a vector).] between two consecutive elements $w(x;i)$ and $w(x;i+1)$ of this combinatorial line is a constant. Let us call this constant $l = (l_0, l_1, \ldots, l_{n-1}) = w(x;i+1) - w(x;i)$.

For $j \in \{0, 1, \ldots, n-1\}$, l_j has two values:

$$l_j = \begin{cases} 1 & \text{if } y_{j,i} \neq y_{j,i+1} \\ 0 & \text{if } y_{j,i} = y_{j,i+1} \end{cases} .$$

Let $w(x;0) = (y_{0,0}, y_{1,0}, \ldots, y_{n-1,0})$ be the first element of the combinatorial line generated by $w(x)$. Then, for $0 \leq i \leq k-1$ an element $w(x;i)$ of the combinatorial line can be expressed as:

$$w(x;i) = w(x;o) + il.$$

[Jan: Change o to 0.]

Let call by a the image of $w(x;0)$ by f, that is $a = f(w(x;0))$ and by d the image of l by f, that is $d = f(l)$. a and d are both integers. We denote by J the set $\{j : \ y_{j,i} \neq y_{j,i+1}\}$. The integer d can be expressed as:

$$d = f(l) = l_0 + l_1 k + \ldots + l_{n-1} k^{n-1} = \sum_{j=0}^{n-1} l_j k^j = \sum_{j \in J} k^j.$$

Thus, $f(w(x;i)) = a + id$, a and d fixed, $0 \leq i \leq k-1$. Hence, the set $\{a + id : \ i \in [k]\}$ forms an arithmetic progression of length k. So, for any combinatorial line of k elements corresponds an arithmetic progression of length k.

Therefore, the Hales-Jewett theorem implies Van der Waerden's theorem. [Jan: Your explanation so far was good, but you are not finished yet. You are proving VdW, so you have k and r. What k and r do you choose for HJ (the same, but you have to say it). What is N_0 that you get for VdW in terms of $HJ(k,r)$?]

2.4.6 Density version of Hales-Jewett theorem implies Szemerédi's theorem. We have shown that any combinatorial line of k elements corresponds an arithmetic progression of length k. Also, we have established that there exists a bijection between $[k]^n \longrightarrow [k^n]$. So, we just need to set $N(k,\delta) = k^n$ to show that the Hales-Jewett theorem implies the Szemerédi's theorem. [Jan: Stil not fixed. What is n here?]

As we have shown that Szemerédi's theorem implies Van der Waerden's theorem, we can establish by transitivity that the density version of Hales-Jewett implies Van der Waerden's theorem.

2.4.7 Density Hales-Jewett number.

2.4.8 Definition. Let $n \geq 0$ and $k \geq 1$. The *density Hales-Jewett number* denoted by $d_{k,n}$

is defined as the size of the largest subset of the set $[k]^n = \{1, 2, \ldots, k\}^n$ which contains no combinatorial line.

If W is the largest subset of $[k]^n$ without a combinatorial line, then $d_{k,n} = |W|$. W is also called a *line-free*. We denote by $\Delta_{k,n} = \frac{|W|}{n^k}$ the density of W.

The combinatorial line is to $\Delta_{k,n}$ for the density Hales-Jewett number [Jan: s/number/theorem] what the arithmetic progression is to $\delta_{k,N}$ for the Szemerédi's theorem. That is, the major difference between $\Delta_{k,n}$ and $\delta_{k,N}$ is located on the definition of the largest subset: combinatorial line for the first and arithmetic progression for the second.

Furstenberg and Katznelson (1991) showed that $d_{k,n} = o(k^n)$ (respectively $r_{k,N} = o(k^n)$) as $n \longrightarrow \infty$. [Jan: Rephrase: Density Hales-Jewett theorem is equivalent to saying that $d_{k,n} = o(k^n)$.] Informally, the little-o means that the upper bound for $d_{k,n}$ (respectively $r_{k,N}$) but that $d_{k,n}$ (respectively $r_{k,N}$) can never be equal to k^n. [Jan: Rephrase: ...it means that $d_{k,n}$ grows slower than any constant fraction of k^n]. In another words, the growth rate of $d_{k,n}$ (respectively $r_{k,N}$) is less [Jan: s/less/strictly less] than the growth rate of k^n.

For $k = 1$ and $k = 2$, the density Hales-Jewett numbers $d_{1,n}$ and $d_{2,n}$ are trivial. [Jan: Don't say it is trivial for $k = 2$. You are not allowed to say it is trivial if you cannot prove it (can you?). You can say that it is easier than other cases.] That is, $d_{1,n} = 1$ and $d_{2,n} = \binom{n}{\lfloor \frac{n}{2} \rfloor}$ where $\lfloor x \rfloor$ is the floor function defined as following: $\lfloor x \rfloor = n \Longleftrightarrow n \leq x < n + 1 \Longleftrightarrow x - 1 < n \leq x$. [Jan: Definition of floor is not correct (you have to say n is integer). You can delete it anyway.]

Polymath (2010) used both human and computer-assisted arguments to compute some non-trivial density Hales-Jewett numbers for $k = 3$ when $n = 0, \ldots, 6$.

$\mathbf{n}$	0	1	2	3	4	5	6
$\mathbf{d_{3,n}}$	1	2	6	18	52	150	450

Table 2.4: Some known values of $d_{3,n}$ for $n = 0, \ldots, 6$.

Let us give examples of the line-free derived from Polymath (2010) for $k = 3$ and $n = 2$ and $n = 3$.

- For $n = 2$, there are 4 largest line-free of $[3]^2$ each with cardinality $d_{3,2} = 6 : \{12, 13, 21, 22, 31, 33\}$, $\{11, 12, 21, 23, 32, 33\}$, $\{11, 13, 22, 23, 31, 32\}$, $\{12, 13, 21, 23, 31, 32\}$.
- For $n = 3$, the largest line-free of $[3]^3$ with cardinality $d_{3,3} = 18$ is: $\{112, 113, 121, 122, 131, 133, 211, 212,$

[Jan: Fix too long lines here.]

Knowing that $d_{3,0} = 1$, $d_{3,1} = 2$, Polymath (2010) gave an upper bound of $d_{3,n}$ for all n:

$$d_{3,n+1} \leq 3d_{3,n}.$$

Polymath (2010) presented some approximations of the lower and upper bounds for general case of $d_{k,n}$. We present these bounds in (4.1.1) for establishing the connection between Hales-Jewett theorem and the parallel repetition of multi-prover games. This connection is developed in the end of the chapter 3.

3. Parallel repetition of multi-prover games.

In this chapter we discuss about the parallel repetition of multi-prover games. Firstly, some notions about two-prover games are presented. Then, a generalisation to multiple provers is given. In the end, these notions are followed by notions about parallel repetition in which is presented the theorem that expresses the upper bound of the value of the success probability of the parallel repetition of multi-prover games.

3.1 Two-prover games.

3.1.1 Definitions. Consider a game G of incomplete information played between two persons cooperative (Player 1 and Player 2) (Verbitsky, 1996; Raz, 2010). A *two-prover one round game* or simply *two-prover game* (often called *game* in this work for short) is a game played between two players called *prover* and an additional player called *verifier* or *referee.* We denote it by $MIP(2,1)$. Notice that a two-prover game is a concept originating from theoretical computer science. Let us introduce some basic idea of this game.

Let X, Y, S, T be finite sets. Let Q be a subset of $X \times Y$ ($Q \subseteq X \times Y$ can represent a set of pair of questions: X represent the set of possible questions for the first prover and Y a set of possible questions for the second prover). S and T can be interpreted respectively as set of possible answers associated respectively to X and Y.

A pair $(x, y) \in_{\mu} Q \subseteq X \times Y$ of questions is chosen randomly by the verifier, that is with a probability distribution measure $\mu : Q \longmapsto \mathbb{R}^{+}$. The verifier sends x to the first prover and y to the second prover. Each prover does not know the question addressed to the other and the communication during the game is not allowed. Nevertheless, before the game starts, they are allowed to agree on a strategy that will help them to increase the probability of winning the game. Let us introduce some main idea of this strategy.

The *strategy* used to answer the pair of questions (x, y) is a pair of functions (f, h) defined as: $f : X \longrightarrow S : x \longmapsto f(x)$ and $h : Y \longrightarrow T : y \longmapsto h(y)$. That is, $f(x) \in S$ is the answer to the question x using the strategy f by prover 1. Whereas $h(y) \in T$ is the answer to the question y using the strategy h by prover 2.

The role of the verifier is to accept or reject the answers given from both provers. Thus, the verifier is also a function. We denote the function "*verifier*" by ϕ and defined as: $\phi : (X, Y, S, T) \longrightarrow \{0, 1\} : (x, y, f(x), h(y)) \longmapsto \phi(x, y, f(x), h(y))$. ϕ is a predicate on (X, Y, S, T).

If $\phi(x, y, f(x), h(y)) = 1$, then the two players win. They lose if $\phi(x, y, f(x), h(y)) = 0$.

In sum, in this case $G = (\phi, Q \subseteq X \times Y, S, T, \mu)$ represents a game if X, Y, S, T are finite subset, the function $\phi : Q \times S \times T \longmapsto \{0, 1\}$ is a predicate, and μ is a probability distribution measure. That is, a prover game is a tuple.

Prover games become interesting when we want to estimate the probability of winning the game according to the strategies used, and mainly when several questions are addressed simultaneously to each prover.

Let $\Pr[\phi(x, y, f(x), h(y)) = 1]$ be the winning probability associated to the one of the couples (f, h) of the strategies. In this case, the winning probability " $\Pr$" which can be the expectation is taken over the distribution μ.

As in all games, the aim of the two players is to maximize the winning probability according to their strategies. Let denote by $\text{val}(G)$ the *value* of the winning probability associated to the optimal couple of strategies of the two provers for the game G where the probability is taken over the couple $(x, y) \in_\mu Q$. Then, $\text{val}(G)$ is expressed as:

$$\text{val}(G) = \max_{f,h} \Pr_{(x,y)\sim Q}[\phi(x, y, f(x), h(y)) = 1]$$

where $\Pr_{(x,y)\sim Q}$ means that the probability is taken over the couple $(x, y) \in_\mu Q$ and $\max_{f,h}$ means that the maximum winning probability is taken over all possible couple of strategies (f, g).

When $\text{val}(G) = 1$, the game G is called *trivial.* In mostly of cases, we will consider a *non-trivial* game , that is a prover game with $\text{val}(G) \neq 1$.

The two-prover game G is called a *free game* if $Q = X \times Y$, that is, questions to players are independent. Another definition of a free game according to Barak, Rao, Raz, Rosen, and Shaltiel (2009) is when the probability distribution of the questions is a product probability distribution, that is $\mu_{XY} = \mu_X \mu_Y$. The probability distribution μ_{XY} is the joint distribution according to which the verifier chooses a pair of questions to the provers. μ_X (respectively μ_Y) the probability distribution for the verifier to choose a question in the set X (respectively Y).

Raz (2010) gave three nice definitions of kinds of prover games: projection game, unique game and XOR game.

A two-prover game G is called *projection game* if for every pair of questions $(x, y) \in X \times Y$ there is a function $f_{x,y} : T \longmapsto S$, such that, for every $a \in S,\ b \in T$, we have: $\phi(x, y, a, b) = 1$ if and only if $f_{x,y}(b) = a$.

The game G is *unique* if for every $(x, y) \in X \times Y$ the function $f_{x,y}$ is a bijection. Hence, a unique game is a particular case of a projection game.

When sets $T, S = \{0, 1\}$, then the unique game is called a *XOR* game. That is, when sets of question are composed only by 0 and 1.

3.1.2 Relationship between graphs and two-prover games.. The relationship between graphs and two-prover games is broad. Thus, in this part we present an elementary relationship by introducing a two-prover game through basic notions of graphs. Some advanced connections are been studied by Laekhanukit (2014); Tamaki (2015); Dinur, Harsha, Venkat, and Yuen (2016).

Let X, Y be two vertex sets of a bipartite graph. $E \subseteq X \times Y$ an edge set, L a label set which can for instance contain some colours. By c_e we denote a set of constraints associated to edge $e \in E$,for example this constraint can be colouring vertices of edge e with different colours chosen in L.

In this case for graphs, a two-prover game G is the game $G = (X, Y, E, L, C)$ where $C = \{c_e\}_{e \in E}$ is the set of (sets of) constraints associated to edges $e \in E$. In others words, a two-prover game G consists of a bipartite graph with vertex sets X, Y, an edge set $E \subseteq X \times Y$, a label set L and a set of constraints associated to edges.

Let us define two functions f and g which assign colours to each vertices $x \in X$ and $y \in Y$ by $f : X \longmapsto L$ and $g : Y \longmapsto L$. We say that f and g satisfy the constraint $c_{(x,y)}$ if $(f(x), g(y)) \in c_{(x,y)}$, that is if $f(x)$ and $g(y)$ satisfy the constraints in $c_{(x,y)}$. So, the value of the game is the success probability to find a couple of functions (f, g) that assigns the maximum of colours. Tamaki (2015) expresses this value as follows:

$$\operatorname{val}(G) = \max_{f,g} \Pr_{(x,y)\sim E} \{(f(x), g(y)) \in c_{(x,y)}\}$$

where the probabilitu is taken over the edge $(x, y) \in E$ and the maximum of probability is taken over all optimal couple of strategies (f, g).

3.1.3 Expander graph. Let us discuss about some elementary notions of *expander graph* which will be useful in the following. These notions are derived mainly from the work of Raz and Rosen (2012). Before giving a definition of what is an expander graph, let us give a short definition of what are a bipartite graph, an unbalanced bipartite graph and a regular graph.

- The graph $G = (U; E) = (X, Y; E)$ is *bipartite*, where the vertex set $U = X \cup Y$ is partionned into two parts X and Y with $E \subseteq X \times Y$.
- The bipartite graph $G = (U; E) = (X, Y; E)$ is *unbalanced* when $|X| \neq |Y|$. Otherwise is *balanced.*
- A graph is regular when each vertex has the same degree, that is each has the same number of neighbours.

Let $U = X \cup Y$ and $E \subseteq X \times Y$ be respectively the set of vertices and the set of edges of a graph G. Let d_X and d_Y be respectively the degree of each vertex $x \in X$ and the degree of each vertex $y \in Y$.

We denote by $(d_X, d_Y)-$bipartite graph an *unbalanced bipartite regular graph* on vertices $X \cup Y$.

Let $G_{XY} = (X, Y, E)$ a bipartite graph. The expander graph G_{XY} is based on the notions of singular values (absolute values of the eigenvalues) of the normalized adjacency matrix $M = M(G_{XY})$ of G_{XY}, that is where each entry of M is divided by $\sqrt{d_X.d_Y}$. The singular-value decomposition theorem states that for an $|X|$-by-$|Y|$ matrix M , there exists a factorisation of the matrix M to the form $M = UDV^*$ where U is an $|X|$-by-$|X|$ unitary matrix ($U^* = U^{-1}$), D is an $|X|$-by-$|Y|$ diagonal matrix with non-negative real numbers on the diagonal and V^* is the conjugate transpose of a $|Y|$-by-$|Y|$ unitary matrix V. The columns of U are eigenvectors of MM^*. The columns of V are eigenvectors of M^*M. The diagonal value in the matrix D are square roots of the eigenvalues of MM^* and M^*M that correspond with the same columns in U and V.

So, a non-negative real number σ is a singular value for the matrix M if and only if there exists two unit-length vectors u and v such that $Mv = \sigma u$ and $M^*u = \sigma v$. The vector u is called left-singular and v right-singular for σ.

In $M = UDV^*$, the diagonal entries of D are equal to the singular values of M. Let us denote by σ_0 the singular value whose absolute value is the largest. The columns of U and V are, respectively, left- and right-singular vectors for the corresponding singular values.

As the matrix M is a normalized matrix, then all singular values are between 0 and 1 , therefore the singular value $\sigma_0 = 1$, that is $u = v$. We denote by $1 - \lambda$ the singular value whose value is the closest to 1 and that is not σ_0. λ is called the *spectral gap* of the graph G_{XY} and $1 - \lambda$ is called the *second singular value*.

Thus, a $(X, Y, d_X, d_Y, 1 - \lambda)-$expander graph is a $(d_X, d_Y)-$bipartite graph with the second singular value $1 - \lambda$ (Raz and Rosen, 2012). That is the expander graph is based on the notions of an unbalanced bipartite regular graph, the set of degrees of his vertices, and on singular value associated to the normalized adjacency matrix of the graph.

[Jan: This is a good exposition of algebraic expander graphs. Since you already wrote about them, it would be useful to explain their graph-theoretic properties (look up Cheeger inequality or expander mixing lemma). Also consider some examples: Is cycle an expander? Is complete graph? Random graph?]

[Jan: Consider separate subsection for expander graphs.]

3.1.4 Multi-prover games.. The rules of the multi-prover games are similar to two-prover games. But, as indicated by the term "multi", this game is playing with several provers (more than two players). That is, we are dealing with the general case.

Let consider that there are $k-$provers, with $k \geq 2$. A $k-$ prover game is the game $G(\phi, Q \subseteq X^1 \times \cdots \times X^k, A^1, \cdots, A^k, \mu)$. So, $k-$tuple of questions $(x^1, \cdots, x^k) \in_\mu Q \subseteq X^1 \times \cdots \times X^k$ (with X^t set of questions) is chosen with probability distribution measure μ from a set of question, and the answer is a $k-$tuple vector $(a^1, \cdots, a^k) \in A^1 \times \cdots \times A^k$ (with A^t set of answers) according to question $(x^1, \cdots, x^k)$. The distribution measure μ associates an element of $Q \subseteq X^1 \times \cdots \times X^k$ to an element of $\mathbb{R}^+ \cap [0, 1] = (0, 1]$. A verifier chooses $k-$tuple of questions $(x^1, \cdots, x^k)$ and sends a question x^t to the prover t. The answer a^t of the prover t depends only on the question x^t. As for two-prover games, the players cannot communicate during the game, but they are allowed to agree on a strategy.

In this case, the strategy used to answer is a $k-$tuple of functions $(f^1, \cdots, f^k)$ defined as: $f^t : X^t \longrightarrow A^t : x^t \longmapsto f^t(x^t) = a^t$, for $1 \leq t \leq k$.

The predicate (verifier) on $(X^1 \times \cdots \times X^k, A^1 \times \cdots \times A^k)$ is defined as a function ϕ:

$$\begin{aligned} \phi :& X^1 \times \ldots \times X^k \times A^1 \times \ldots \times A^k \longmapsto \{0, 1\} \\ & (x^1, \cdots, x^k, f^1(x^1), \cdots, f^k(x^k)) \longmapsto \phi(x^1, \cdots, x^k, f^1(x^1), \cdots, f^k(x^k)). \end{aligned}$$

All players win if $\phi(x^1, \cdots, x^k, f^1(x^1), \cdots, f^k(x^k)) = 1$.

Thus, the value of the multi-prover game G denoted by $\mathrm{val}(G)$ is the optimal winning probability of provers over all possible strategies. This value is expressed as follows:

$$\mathrm{val}(G) = \max_{f^1,\cdots,f^k} \Pr[\phi(x^1,\cdots,x^k, f^1(x^1),\cdots,f^k(x^k)) = 1].$$

Some notions on multi-prover games presented above mainly treat on one round. We can extend this concept from one round to several rounds. Thus, the $k-$provers $r-$round game is similar to the multi-prover with k players, but in this case the verifier executes a computation at most r rounds following a game.

3.1.5 Some types of prover games.. In the table (3.1), we present some kinds of the prover game known. We give some references for further reading.

Prover game	**References**
Free	Verbitsky (1996)
Projection	Rao (2011)
Unique	Tamaki (2015)
Expander	Dinur et al. (2016)
Anchored	Bavarian et al. (2015)
GHZ	Dinur et al. (2016)
Fortified	Moshkovitz (2014)
XOR	Cleve et al. (2007)
Question set	Hązła et al. (2016)

Table 3.1: Some kinds of prover games.

3.2 Parallel repetition.

3.2.1 Parallel repetition for two-prover games. Let G be a two-prover game and n a positive integer. Knowing the value of the game G, we are interesting to establish the relationship between $\mathrm{val}(G)$ and $\mathrm{val}(G^n)$. By executing n independent copies of G in parallel, we obtain what we call an $n-$*product game G* or a *product game* G^n or an *n-fold parallel repetition* G^n. Hence, a parallel repetition of a two-prover game G is a product game G^n, that is approximatively speaking when n copies of the game G is tried to be won simultaneously by the two players. The game G is called the *base game* of the parallel repeated game G^n.

According to the definition of a prover G, let $G(\phi, Q \subseteq X \times Y, S, T, \mu)$ be a game. The product game G^n is the game $G^n(\phi^n, Q^n \subseteq X^n \times Y^n, S^n, T^n, \mu^n)$, where ϕ^n represents a predicate (referee or verifier), Q^n a product set of questions, S^n and T^n represent sets of answers, and μ^n represents the probability distribution measure. Let us express explicitly the sets Q^n and the functions μ^n and ϕ^n.

Elements of Q^n take the form $((x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n))$ where $x_1, x_2, \ldots, x_n \in X$ and $y_1, y_2, \ldots, y_n \in Y$, that is a collection of $n-$tuple of couples $((x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n))$

is chosen randomly and uniformly from the set Q^n in accordance with the probability distribution measure μ^n. The element $((x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)) \in Q^n$ is identifying to the pair $((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \in Q^n \subseteq X^n \times Y^n$.

Thus, the probability measure μ^n can be expressed as a function using μ:

$$\begin{aligned}\mu^n :& Q^n \subseteq X^n \times Y^n \longrightarrow \mathbb{R}^+\\ &((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \longmapsto \mu^n((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \prod_{i=1}^{n} \mu(x_i, y_i).\end{aligned}$$

We denote by $\bar{x}$ the $n-$tuple $(x_1, \ldots, x_n)$, that is $\bar{x} = (x_1, \ldots, x_n)$.

The function ϕ^n is defined similarly to the function ϕ as:

$$\begin{aligned}\phi^n :& X^n \times Y^n \times S^n \times T^n \longrightarrow \{0, 1\}\\ &(\bar{x}, \bar{y}, \bar{s}, \bar{t}) \longmapsto \phi^n(\bar{x}, \bar{y}, \bar{s}, \bar{t}) = \bigwedge_{i=1}^{n} \phi[x_i, y_i, f_i(\bar{x}), h_i(\bar{y})]\end{aligned}$$

Where $\bigwedge$ represents the logical connective "AND" (conjunction). Note that f_i is a function of $\bar{x}$ and not just x_i in the expression of the predicate ϕ^n.

We know that in the truth table for the logical operator "AND", the only case so that the value of two propositions be true is when the two propositions are true. Then, the logical connective $\bigwedge$ from ϕ^n can be replaced by $\prod$. That is, $\bigwedge\limits_{i=1}^{n} \phi[x_i, y_i, f_i(\bar{x}), h_i(\bar{y})] = \prod\limits_{i=1}^{n} \phi[x_i, y_i, f_i(\bar{x}), h_i(\bar{y})]$.

As there are two provers, n-vectors (questions) are revealed to each prover: $(x_1, \ldots, x_n)$ to prover 1 and $(y_1, \ldots, y_n)$ to prover 2 who both respond with couple of strategies (F, H) with $F = (f_1, f_2, \ldots, f_n)$ and $H = (h_1, h_2, \ldots, h_n)$ where f_i and h_i represent respectively strategies associated to the questions $\bar{x}$ and $\bar{y}$.

Strategies F and H are functions defined as:

$$\begin{aligned}F :& X^n \longrightarrow S^n\\ &\bar{x} \longmapsto F(\bar{x}) = (f_1(\bar{x}), \ldots, f_n(\bar{x}))\end{aligned}$$

and

$$\begin{aligned}H :& Y^n \longrightarrow T^n\\ &\bar{y} \longmapsto H(\bar{y}) = (h_1(\bar{y}), \ldots, h_n(\bar{y}))\end{aligned}$$

Now, the winning case occurs when $\bigwedge\limits_{i=1}^{n} \phi[x_i, y_i, f_i(\bar{x}), h_i(\bar{y})] = 1$, that is both provers win if they win concomitantly in all n coordinates. Each of the n copies are treated independently by the referee.

Then, the value of the game G^n, that is the success probability is:

$$\mathrm{val}(G^n) = \max_{F,H} \Pr\left[\bigwedge_{i=1}^{n} \phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1\right].$$

The winning probability of G^n and the one of G are linked by these relations:

$$\mathrm{val}(G)^n \leq \mathrm{val}(G^n) \leq \mathrm{val}(G). \tag{3.2.1}$$

Let us show the inequalities in (3.2.1) by splitting them into two parts:

$$\begin{cases} \mathrm{val}(G)^n \leq \mathrm{val}(G^n) \\ \mathrm{val}(G^n) \leq \mathrm{val}(G). \end{cases} \tag{3.2.2}$$

- The first inequality $\mathrm{val}(G)^n \leq \mathrm{val}(G^n)$.

  Proof. We know that the value of the game G is the optimal winning probability of provers over all possible strategies, that is the winning probability using the best couple of strategies. Le us denote by (f, h) this optimal couple of strategies used for the game G. Strategies f and h are defined as $f : X \longrightarrow S$ and $h : Y \longrightarrow T$. Then, $\mathrm{val}(G) = \max\limits_{f,g} \Pr[\phi(x, y, f(x), h(y)) = 1]$.

  As far as, let us denote by (F, H) a couple of strategies used to win the game G^n. F and G are $n-$tuple defined as: $F = (f_1, \dots, f_n)$ and $H = (h_1, \dots, h_n)$. Strategies F and H are defined as $F : X^n \longrightarrow S^n$ and $H : Y^n \longrightarrow T^n$. Here, notice that the couple (F, H) of strategies are not necessary the optimal. Then, the winning probability according to this couple of strategies is: $\Pr\left[\bigwedge_{i=1}^{n} \phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1\right]$.

  Since, each couple (x_i, y_i), for $1 \leq i \leq n$ is chosen randomly according to the probability distribution measure μ. Without loss of generality, for instance, let us assume that the couple (x_i, y_i) is chosen independently. Then, the winning probability becomes:

$$\Pr\left[\bigwedge_{i=1}^{n} \phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1\right] = \prod_{i=1}^{n} \Pr\left[\phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1\right].$$

  Let us chose the optimal strategies f and h of G to play each parallel copy of G, that is $f_i(\bar{x}) = f(x_i)$ and $h_i(\bar{y} = h(y_i)$ for $1 \leq i \leq n$. Then, the success probability becomes:

$$\begin{aligned} \Pr\left[\bigwedge_{i=1}^{n} \phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1\right] &= \prod_{i=1}^{n} \Pr\left[\phi(x_i, y_i, f(\bar{x}), h(\bar{y})) = 1\right] \\ &= \prod_{i=1}^{n} \mathrm{val}(G) \\ &= \mathrm{val}(G)^n. \end{aligned}$$

  (f, h) is the optimal couple of strategies for the game G, this does not means that the couple (F, H) is the optimal couple of the strategies for the parallel repetition G^n. Then, the winning probability for G^n over the optimal couple of strategies is:

$$\begin{aligned}\mathrm{val}(G^n) =& \max_{F,H} \Pr\left[\bigwedge_{i=1}^{n} \phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1\right] \\ \geq& \Pr\left[\bigwedge_{i=1}^{n} \phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1\right] \\ =& \prod_{i=1}^{n} \Pr\left[\phi(x_i, y_i, f(\bar{x}), h(\bar{y})) = 1\right] \\ =& \prod_{i=1}^{n} \mathrm{val}(G) \\ =& \mathrm{val}(G)^n.\end{aligned}$$

Hence, $\mathrm{val}(G^n) \geq \mathrm{val}(G)^n$. □

- The second inequality: $\mathrm{val}(G^n) \leq \mathrm{val}(G)$.

  Proof.

$$\begin{aligned}\mathrm{val}(G^n) &= \max_{F,H} \Pr\left[\bigwedge_{i=1}^{n} \phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1\right] \\ &\leq Pr\left[\phi(x_1, y_1, f_1(\bar{x}), h_1(\bar{y})) = 1\right] \\ &\leq \max_{f,g} \Pr[\phi(x_1, y_1, f(x), h(y)) = 1] \\ &= \mathrm{val}(G).\end{aligned}$$

  Hence, $\mathrm{val}(G^n) \leq \mathrm{val}(G)$. □

To support the relation $\mathrm{val}(G)^n \leq \mathrm{val}(G^n) \leq \mathrm{val}(G)$, let us give an example for which we define a strategy.

Let G be a two-prover game and $X = Y = \{0, 1\}$ be sets of questions addressed respectively to prover A and B. The rule of the game G is announced as this. The verifier ϕ chooses randomly and uniformly a couple of questions $(x, y) \in Q = X \times Y = \{(0, 0); (0, 1); (1, 0); (1, 1)\}$ and sends x to the prover A and y to the prover B. The sets of answers of the two provers are respectively $S = \{(a, K_A)\}$ and $T = \{(b, K_B)\}$ where $a, b \in \{0, 1\}$, $K_A, K_B \in \{A, B\}$. Note that $|S| = |T| = 4$. To win, the verifier checks this:

- $K_A = K_B = K$ and $a = b$.
- If $K = A$, then $x = a$, that is, if both provers answer A then the first component of he couple of answers of the provers is $x = a = b$.
- If $K = B$, then $y = b$, that is, if both provers answer B then the first component of he couple of answers of the provers is $y = a = b$.

This means that the winning cases are: $\phi[x, y, (x, A), (x, A)]$ and $\phi[x, y, (y, B), (y, B)]$.

Let us define a couple of strategies (f, g) used by the two players to answer as following: $f(0) = (0, A), f(1) = (1, A)$ and $g(0) = (0, A), g(1) = (1, A)$. Let us evaluate the probability to win this game. In our strategy, we always have $K_A = K_B = A$ in the second component of the answer. So, the two provers can win in two cases: $(0, 0)$ and $(1, 1)$. They also lose in two cases: $(0, 1)$ and $(0, 1)$. Hence, the winning probability of the game according to this couple of strategies is: $\Pr[\phi(x, y, (a, K_A), (b, K_B)) = 1] = \frac{2}{4} = \frac{1}{2}$.

Let us define another couple of strategies (s, t) such that $s(0) = (0, A), s(1) = (0, A)$ and $t(0) = (0, A), t(1) = (0, A)$. For this couple of strategies, the two provers can win in two cases: $(0, 0)$ and $(0, 1)$. They also lose in two cases: $(1, 0)$ and $(1, 1)$. Hence, the winning probability of the game according to this couple of strategies is: $\Pr[\phi(x, y, (a, K_A), (b, K_B)) = 1] = \frac{2}{4} = \frac{1}{2}$.

For all possible couple of strategies, the maximum value of the winning probability is $\frac{1}{2}$. Therefore, the value of the game G is:

$$\mathrm{val}(G) = \frac{1}{2}.$$

Now, let us compute $\mathrm{val}(G^2)$. Firstly, let us define the game G^2.

The sets of questions are respectively $X^2 = Y^2 = \{(0, 0); (0, 1); (1, 0); (1, 1)\}$. The verifier chooses randomly and uniformly the couple $(\bar{x}, \bar{y}) \in Q = X^2 \times Y^2 = \{(\bar{x}, \bar{y}) : \bar{x} \in X^2, \bar{y} \in Y^2\} = \{((0, 0), (0, 0)), \ldots, ((1, 1), (1, 1))\}$ where $\bar{x} = (x_1, x_2)$ and $\bar{y} = (y_1, y_2)$ are couples with $x_1, x_2, y_1, y_2 \in \{0, 1\}$. Note that $|Q| = 16$. The sets of answers are :$S^2 = \{(\bar{s}_1, \bar{s}_2) : \bar{s}_1, \bar{s}_2 \in S\} = \{((a, K_A), (a, K_A)) : a \in \{0, 1\}, K_A \in \{A, B\}\}$ and $T^2 = \{(\bar{t}_1, \bar{t}_2) : \bar{t}_1, \bar{t}_2 \in T\} = \{((b, K_B), (b, K_B)) : b \in \{0, 1\}, K_B \in \{A, B\}\}$. The verifier sends $\bar{x}$ to prover A and $\bar{y}$ to prover B. Answers of $\bar{x}$ is in S^2 and answers of $\bar{y}$ is in T^2. The verifier checks these rules:

- If $x_1 = y_2$ then both provers A and B win.
- If $x_1 \neq y_2$ then they lose.

For that, let us define a couple of strategies (h, k) such that $h(\bar{x}) = h(x_1, x_2) = ((x_1, A), (x_1, B))$ and $k(\bar{y}) = k(y_1, y_2) = ((y_1, A), (y_2, B))$.

According to this couple of strategies, both provers A and B win in these cases:

A	(0,0)	(0,0)	(0,1)	(0,1)	(1,0)	(1,0)	(1,1)	(1,1)
B	(0,0)	(1,0)	(0,0)	(1,0)	(0,1)	(1,1)	(1,1)	(0,1)

And they lose in these cases:

A	(0,0)	(0,0)	(0,1)	(0,1)	(1,0)	(1,0)	(1,1)	(1,1)
B	(0,1)	(1,1)	(0,1)	(1,1)	(0,0)	(1,0)	(0,0)	(1,0)

Then, the winning probability of the game G^2 according to the couple of strategies (h, k) is $\frac{8}{16} = \frac{1}{2}$.

For all couple of strategies, we assume that the winning probability is less or equal to $\frac{1}{2}$.

Thus, the value of the game G^2 is:

$$\mathrm{val}(G^2) = \frac{1}{2}.$$

Therefore, $\mathrm{val}(G)^2 \leq \mathrm{val}(G^2) \leq \mathrm{val}(G)$.

3.2.2 Parallel repetition theorem of two-prover games.. The parallel repetition theorem of two-prover games present an approximation upper bound of the value of n independent copies of the game G. Many main topics on the parallel repetition of prover game started to be treated from the early 1990s.

Feige and Lovász (1992) conjectured that for any two-prover game G with value smaller than 1 ($\mathrm{val}(G) < 1$), the value of the game G^n ($\mathrm{val}(G^n)$ decreases exponentially fast to 0.

We denote by $|S|$ and $|T|$ respectively the size of the sets of answers S and T of the game G. Thus, the answer size of the game G is $|S||T|$. Let us denote by c a universal constant and by s the expression $s(G) = \log |S||T|$ which represents the length of the answers. s can also represent the answer size. The parallel repetition theorem as formulated in Raz (1998, 2010) is stated as follows:

3.2.3 Theorem. *For any two-prover game G, with $\mathrm{val}(G) \leq 1 - \epsilon$, for $0 < \epsilon \leq 1$, the value of the game G^n is:*

$$\mathrm{val}(G^n) \leq (1 - \epsilon^c)^{\Omega(n/s)}.$$

Knowing that for all real number, $1 + x \leq e^x$ and for x closer to zero: $e^x = 1 + x + O(x^2)$ or simply $1 + x \approx e^x$, the bound of $\mathrm{val}(G^n)$ as expressed in (3.2.3) can be rewritten as follows:

$$\begin{aligned}\mathrm{val}(G^n) \leq& (1 - \epsilon^c)^{\Omega(n/s)} \\ \leq& \left(e^{-\epsilon^c}\right)^{\Omega(n/s)} \\ =& \exp(-\epsilon^c \Omega(n/s)).\end{aligned}$$

Then, $\mathrm{val}(G^n) \leq \exp(-\epsilon^c \Omega(n/s))$. Or

$$\begin{aligned}\mathrm{val}(G^n) \leq& \exp(-\epsilon^c \Omega(n/s)) \\ =& \exp(-\epsilon \epsilon^{c-1} \Omega(n/s)) \\ =& \exp(-\epsilon)^{\epsilon^{c-1}\Omega(n/s)} \\ \approx& (1 - \epsilon)^{\epsilon^{c-1}\Omega(n/s)}.\end{aligned}$$

Then, $\mathrm{val}(G^n) \leq (1 - \epsilon)^{\epsilon^c \Omega(n/s)}$.

In some papers, the authors, for instance Rao (2011) expresses the upper bound of $\mathrm{val}(G^n)$ by using this expression: $\mathrm{val}(G^n) \leq (1 - \epsilon/2)^{\epsilon^c \Omega(n/s)}$.

Feige and Lovász (1992) conjectured the parallel repetition theorem and gave some proofs for some special cases. The proof of the theorem (3.2.3) has been given by Raz (1998) and found an implicit constant $c = 32$. Holenstein (2007) simplified Raz's proof, proved the parallel repetition theorem in case of no-signaling strategies (strategies which do not imply communication) and gave an explicit bound on the maximal success probability of the product game G^n. This explicit bound is expressed as:

$$\mathrm{val}(G^n) \leq \left(1 - \frac{(1 - \mathrm{val}(G))^3}{6000}\right)^{\frac{n}{\log(|A||B|)}}$$

. This means that the constant $c = 3$ in Thomas Holenstein's bound which is better than Ran Raz's expression. However, for the special case of the projection games. Rao (2011) improved the bound of this game by finding $c = 2$ and by expressing the function Ω without s. This bound is:

$$\mathrm{val}(G^n) \leq (1 - \epsilon^2)^{\Omega(n)}.$$

According to Raz (2010), this bound was also known for the special case of XOR games.

To improve this bound from (3.2.3) to $(1-\epsilon)^{\Omega(n/s)}$ for the $n-$product game of two-prover games or for some special cases is one of the questions for which several researchers are looking for answers (Raz, 2010). This question is called the *strong parallel repetition problem*.

In case if the probability distribution on $X \times Y$ is a product distribution for games , Barak et al. (2009) showed that the value of free game is bounded as follows:

$$\mathrm{val}(G^n) \leq (1 - \epsilon^2)^{\Omega(n/s)}$$

and if the game is a free projection game, then the value of the game is:

$$\mathrm{val}(G^n) \leq (1 - \epsilon)^{\Omega(n)}.$$

Hence, the strong parallel repetition for the free projection game that is with product distribution is known. Note that the function Ω is not depending on s.

Similarly, Raz and Rosen (2012) studied the case where the probability distribution is uniform over the edges of an expander graph. The value of the repeated game is:

$$\mathrm{val}(G^n) \leq (1 - \epsilon^2)^{c(\lambda).\Omega(n/s)}$$

where λ is the normalized spectral gap of the expander graph.

If in addition the game is a projection game, then the value of the repeated game is:

$$\mathrm{val}(G^n) \leq (1 - \epsilon)^{c(\lambda).\Omega(n)}$$

which is a strong parallel repetition for a projection games on expander graph.

However, Raz (2011) gave a negative answer to the several research who are asking if it is possible to found a strong parallel repetition for two-prover games, that is to improve the bound value to $(1 - \epsilon)^{\Omega(n/s)}$. A counterexample to strong parallel repetition used to disprove is an *odd cycle game* of size m which is a two-prover game with value $1 - 1/2m$. Thus, Raz showed that the value of the parallel repetition of this odd cycle game is at least $1-(1/m).O(\sqrt{n})$. Hence, for large $n=\Omega(m^2)$, the value of the parallel repetition (n times) of this odd cycle game is at least $(1-1/4m^2)^{O(n)}$. That is, the lower bound value of parallel repetition of two-prover games is at least $(1-\epsilon^2)^{O(n)}$ and can not reach $(1-\epsilon)^{\Omega(n/s)}$.

Since the odd cycle game is a projection game, a unique game, and a XOR game, this answers negatively most variants of the strong parallel repetition problem (Raz, 2011; Raz and Rosen, 2012). That is there exists a two-prover game (odd cycle game) which does not have a strong parallel repetition theorem.

Moreover, Dinur and Steurer (2014) used projection games to study parallel repetition by using analytical approach based on a matrix analysis argument. His result states that for every projection game G with $\mathrm{val}(G)\le\rho$, we have:

$$\mathrm{val}(G^n)\le\left(\frac{2\sqrt{\rho}}{1+\rho}\right)^{n/2}. \tag{3.2.3}$$

Dinur and Steurer (2014) establishes that this upper value bound (3.2.3) of an $n-$ fold parallel repetition of projection games G and $(1-\epsilon^2)^{O(n)}$ with improved bounds from Rao (2011) match when the value of the game G is closed to 1.

Notice that the good things of those approximations of the upper value of the parallel repetition, is that, the value of the game G^n is reduced exponentially.

In this work, we are mainly interested by the upper bound of the value of the parallel repetition. However, there exists some works which approximate the lower bound (Feige et al., 2007; Steurer, 2010; Raz, 2011). The table (3.2) adapted from Tamaki (2015) presents a summary of lower and upper bounds known of parallel repetition of some two-prover games.

Upper bounds of the value of G^n	Kind of game G	References
$(1-\epsilon^33)^{\Omega(n/s)}$	All provers	Raz (1998)
$(1-\epsilon^3)^{\Omega(n/s)}$	All provers	Holenstein (2007)
$(1-\epsilon^2)^{\Omega(n)}$	Projection, xor	Rao (2011); Raz (2010)
$\left(\frac{2\sqrt{\rho}}{1+\rho}\right)^{n/2}$	Projection	Dinur and Steurer (2014)
$(1-\epsilon^2)^{\Omega(n/s)}$	Free	Barak et al. (2009)
$(1-\epsilon)^{\Omega(n)}$	Free projection	Barak et al. (2009)
$(1-\epsilon^2)^{c(\lambda).\Omega(n/s)}$	Expander with spectral gap λ	Raz and Rosen (2012)
$(1-\epsilon)^{c(\lambda).\Omega(n)}$	Projection on Expander games	Raz and Rosen (2012)

Lower bounds of the value of G^n	Kind of game G	Reference
$1-(1/m).O(\sqrt{n})$	Odd cycle, value $1-1/m$	Feige et al. (2007)
$(1-1/4m^2)^{O(n)}$	Odd cycle, $n\ge\Omega(m^2)$	Raz (2011)
$1-O(\sqrt{\epsilon ns})$	Unique	Steurer (2010)

Table 3.2: Summary of known bounds

3.2.4 Parallel repetition of mutli-prover games. Let $G(\phi, Q \subset X^1 \times \ldots \times X^k, A^1, \ldots, A^k, \mu)$ be a $k-$prover game, that is a prover game played with k players. For $1 \leq t \leq k$, the sets X^t and A^t represent respectively the set of questions and the set of their answers. The verifier ϕ is a predicate defined on $\left(\prod_{t=1}^{k} X^t, \prod_{t=1}^{k} A^t\right)$, that is $\phi[(x^1, \cdots, x^k), (a^1, \cdots, a^k)] = 1$ for a winning case and the other for the losing case. The distribution measure μ is a function defines from Q to $(0, 1]$.

The $n-$fold parallel repetition of the game G is the $k-$prover game $G^n(\phi^n, Q^n \subseteq (X^1)^n \times \ldots \times (X^k)^n, (A^1)^n, \ldots, (A^k)^n, \mu^n)$, where $(X^1)^n, \ldots, (X^k)^n$ are sets of $n-$tuple of questions, $(A^k)^n, \ldots, (A^k)^n$ are sets of $n-$tuple of answers.

Let us denote by x_i^t a element of the set X^t where superscripts $1 \leq t \leq k$ denote the players and subscripts $1 \leq i \leq n$ denote coordinates in parallel repetition.

Elements of Q^n are n-tuple of $k-$tuple (of questions). $((x_1^1, \cdots, x_1^k), (x_2^1, \cdots, x_2^k), \ldots, (x_n^1, \cdots, x_n^k)) \in_{\mu^n} Q^n$ which is identifying to the $k-$tuple $((x_1^1, \cdots, x_n^1), (x_1^2, \cdots, x_n^2), \ldots, (x_1^k, \cdots, x_n^k))$. Elements of Q^n are chosen randomly in accordance with the probability distribution μ^n. Let $\bar{x}^t$ represent a $n-$tuple $(x_1^t, \cdots, x_n^t)$ belongs to $(X^t)^n$. So, the distribution measure μ^n is a function defined as:

$$\begin{aligned} \mu^n : & Q^n \subseteq (X^1)^n \times \ldots \times (X^k)^n \times \longrightarrow (0, 1] \\ & (\bar{x}^1, \ldots, \bar{x}^k) \longmapsto \mu^n(\bar{x}^1, \ldots, \bar{x}^k) = \prod_{i=1}^{n} \mu(x_i^1, \cdots, x_i^k). \end{aligned}$$

And the verifier is a predicative defines as follows:

$$\begin{aligned} \phi^n : & (X^1)^n \times \ldots \times (X^k)^n \times (A^1)^n \times \ldots \times (A^k)^n) \longrightarrow \{0, 1\} \\ & (\bar{x}^1, \ldots, \bar{x}^k, \bar{a}^1, \ldots, \bar{a}^k) \longmapsto \phi^n(\bar{x}^1, \ldots, \bar{x}^k, \bar{a}^1, \ldots, \bar{a}^k) = \bigwedge_{i=1}^{n} \phi[x_i^1, \cdots, x_i^k, f_i^1(\bar{x}^1), \cdots, f_i^k(\bar{x}^k)] \end{aligned}$$

where $\bigwedge$ represents the logical connective "AND" (conjunction) and f_i^t are strategies.

There are two results: win or lose. All k provers win when $\bigwedge_{i=1}^{n} \phi[x_i^1, \cdots, x_i^k, f_i^1(\bar{x}^1), \cdots, f_i^k(\bar{x}^k)] = 1$, that is when all provers win simultaneously in all n coordinates. The verifier treats independently each of the n copies.

As all provers are allowed to agree on a strategy but not to communicate each other during the game, the strategy in this case is a $k-$tuple of functions $(F^1, F^2, \ldots, F^k)$ where for $1 \leq t \leq k$, every F^t is a $n-$tuple function $(f_1^t, f_2^t, \ldots, f_n^t)$. f_i^t is strategy used by the prover t to give the answer a_i^t of the question x_i^t for $1 \leq i \leq n$. This function f_i^t is defined as:

$$\begin{aligned} f_i^t : & (X^t)^n \longrightarrow A^t \\ & \bar{x}^t \longmapsto f_i^t(\bar{x}^t) = a_i^t \end{aligned}$$

Thus, the value of the parallel repetition of the multi-prover game G denoted by $\mathrm{val}(G^n)$ is the optimal winning probability of provers over all possible strategies. This value is expressed as follows:

$$\mathrm{val}(G^n) = \max_{F^1,F^2,\ldots,F^t} \Pr\left[\bigwedge_{i=1}^{n} \phi\left(x_i^1,\cdots,x_i^k, f_i^1(\bar{x}^1),\cdots,f_i^k(\bar{x}^k)\right) = 1\right].$$

Given the value of the multi-prover game G, can we estimate or approximate the value of the parallel repetition of the multi-prover game G using the value of G?

For a two-prover game, there are so many advanced studies about that, we can cite the works of Feige and Lovász (1992); Verbitsky (1996); Raz (1998); Holenstein (2007); Barak et al. (2009); Raz (2010); Rao (2011); Dinur and Steurer (2014). Nevertheless, express $\mathrm{val}(G^n)$ in terms of power of $\mathrm{val}(G)$ or bound it with the power of $\mathrm{val}(G)$ does not seem to be easy.

Another question that we can ask is: does the value of parallel repetition of a multi-prover game decay exponentially like for a two-prover game?

For some multiplayer games, for instance free game and anchored[1] game, the exponentially decay bounds for parallel repetition are known (Barak et al., 2009; Bavarian et al., 2015). A recent work of Dinur et al. (2016) gives an exponentially decay bound for the parallel repetition for expander games.

Expander game is based on expander graph (see (3.1.2)). Given a base game G, a related connected graph G, a spectral gap of the graph G denoted by λ, then the value of the repeated game, $\mathrm{val}(G^n)$ goes down exponentially in n for sufficiently large n. Dinur et al. (2016) expresses it as follows:

$$\mathrm{val}(G^n) \leq \exp\left(-\frac{c\epsilon^5\lambda^2 n}{\log|A|}\right) \tag{3.2.4}$$

where $|A|$ is the answer size of the game and c a constant.

An expander game is merely the extension of free and anchored games. All kind of expander games are linked by the connectedness property. Hence, the free and anchored games are connected games.

As $0 < \epsilon \leq 1$, ϵ^5 is very smaller than ϵ. The upper bound value (3.2.4) of the parallel repetition of the expander game can be expressed as:

$$\begin{aligned}\mathrm{val}(G^n) &\leq \exp\left(-\frac{c\epsilon^5\lambda^2 n}{\log|A|}\right)\\ &= \exp\left(-\epsilon^5\right)^{\frac{c\lambda^2 n}{\log|A|}}\\ &= \left(1-\epsilon^5\right)^{\frac{c\lambda^2 n}{\log|A|}}\\ &= \left(1-\epsilon^5\right)^{\Omega(n/s)}\end{aligned}$$

where $s = \log|A|$ and $\Omega(n/s) = \frac{c\lambda^2 n}{\log|A|}$ with λ a constant.

[1] Related to quantum parallel repetition. Before being repeated in parallel, the base game G is modified to an equivalent game $\tilde{G}$.

A general bound of the value of parallel repetition of a multi-prover game is given by Verbitsky (1996) by using the Hales-Jewett theorem. Despite the fact that the rate of convergence of this general bound value of Oleg Verbitsky is slow, this boundary remains the only best result that gives a general parallel repetition bound for all multiplayer games (Hązła et al., 2016; Dinur et al., 2016). In the next chapter, we present the connection between Hales-Jewett theorem and the parallel repetition of multi-prover games.

4. Connection between parallel repetition of multi-prover games and Hales-Jewett theorem.

This chapter presents the relationship between parallel repetition of multiple provers with the density Hales-Jewett theorem. We give a parallel repetition bound using the density Hales-Jewett. Firstly, we show that the density Hales-Jewett theorem implies parallel repetition. Secondly, we show that the parallel repetition implies the density Hales-Jewett theorem.

4.1 Hales-Jewett theorem implies parallel repetition.

In both versions of Hales-Jewett theorem (see (2.4.2) and (2.4.3)), the concept which emphasizes this theorem is the *combinatorial line.* The combinatorial line is the umbilical cord between the Hales-Jewett theorem and the parallel repetition. In section (2.4), we have already explain deeply [Jan: s/deeply/in a detailed way] and define what the combinatorial is. Let us recall some notions about a combinatorial line and the formulation of the Hales-Jewett theorem.

Let $k, n \in \mathbb{Z}^+$, $[k] = \{1, 2, \ldots, k\}$ and an $x-$string $w(x) = a_1a_2\ldots a_n \in ([k] \times \{x\})^n \backslash [k]^n$. That is, in $w(x) = a_1a_2\ldots a_n$, at least one of the symbol a_i contains the symbol x called wildcard. Let $w(x; i)$ be the string obtained by replacing x by i.

The *combinatorial line* is the set of k strings $\{w(x; i) \ : \ i \in \{1, 2, \ldots, k\}\}$, that is the set $\{w(x; 1), w(x; 2), \ldots, w(x; k)\}$.

So, in (2.4.2) the Hales-Jewett theorem is given. [Jan: Don't start sentence with "So". You can say "HJ theorem is given in ()".] As the name stipulates, the Hales-Jewett was proved by Hales and Jewett. The formulation is based on colouring of a set and on the existence of s a monochromatic combinatorial line.

Furthermore, there is a density formulation of Hales-Jewett theorem on which this section is mainly constructed. Given a subset A of $[k]^n$, the density of A is defined and denoted as $\delta(A) = \frac{|A|}{k^n}$. By simplicity, δ denotes the density of A, that is $\delta = \delta(A)$.

Thereby, the density version of Hales-Jewett theorem states that for any positive number k and real number δ, there exists a large enough number n (depending on k and δ) such that any subset of $[k]^n$ with density δ contains a combinatorial line. In the following, essentially we use the density version of Hales-Jewett theorem. Whenever there is Hales-Jewett theorem, it means the density version of Hales-Jewett theorem. [Jan: s/Whenever there is/Whenever we say]

We denote by $\Delta_{k,n}$ the maximum density of a subset W of $[k]^n$ without a combinatorial line. We have discussed a lot on this in (??). [Jan: Ref is broken. s/We have discussed a lot/Delta_kn was discussed in] The number $\Delta_{k,n}$ is called density Hales-Jewett number.

The theorem thereafter has been formulated and demonstrated by Hillel Furstenberg and Yitzhak Katznelson during their work on a density version of Hales-Jewett theorem. [Jan: It is still misleading. It was not demonstrated "during their work on DHJ". It *is* the DHJ! I mean it is easy to see that it is equivalent to Theorem 2.4.2. Please say this.]

4.1.1 Theorem (Furstenberg and Katznelson (1991)). *For $k \geq 2$, $\lim\limits_{n \longrightarrow \infty} \Delta_{k,n} = 0$.*

This theorem states that for $k \geq 2$, the maximum density of a subset of $[k]^n$ without a combinatorial line converges to 0 when n converges to infinity. That is, the set $[k]^n$ [Jan: s/the set/a subset of $[k]^n$ with constant measure] will almost necessary [Jan: almost necessary/necessarily] contains a subset with a combinatorial line when n increases.

The proof of this theorem has been given by Furstenberg and Katznelson (1991) without explicit bounds. Polymath (2012) gave an upper bound of $\Delta_{k,n}$ for a particular case ($k = 3$): $\Delta_{3,n} \leq O(1/\sqrt{\log^* n})$. Previously, a lower density Hales-Jewett bound was known through the work of Polymath (2010) who establishes that for $k \geq 3$, $\Delta_{k,n} \geq \exp\left(-O(\log n)^{1/l}\right)$ where ℓ is the largest integer such that $2k > 2^\ell$. This lower bound can simply be written as: $\Delta_{k,n} \geq \exp\left(-O(\log n)^{1/\lceil \log_2 k \rceil}\right)$ where $\lceil x \rceil$=ceilling(x) is the least integer greater than or equal to x. For $k = 2$, the density Hales-Jewett number is: $\Delta_{2,n} = \Theta(1/\sqrt{n})$ known by Sperner's theorem. [Jan: This paragraph belongs to previous chapter.] '

Hillel Furstenberg and Yitzhak Katznelson's theorem (4.1.1) and the Raz theorem (3.2.3) are close but not equivalent. Let us recall what Raz theorem is. The Raz theorem (3.2.3) has been conjectured by Feige and Lovász (1992) and demonstrated by Raz (1998). This conjecture states that the value of a parallel repetition of a game (non trivial) decreases exponentially fast to 0 when n converges to infinity. It is clear that the convergence of Raz theorem is fast than the convergence of Hillel Furstenberg and Yitzhak Katznelson's theorem. Thus, the Raz theorem appears to be bounded by the density of the largest subset without a combinatorial line. [Jan: No, it is not. The theorems are uncomparable. If you take very large answer alphabet size Raz becomes useless while Verbitsky still works. If you take constant alphabet size and epsilon Raz theorem is much faster.] The following Oleg Verbitsky theorem shows that the density Hales-Jewett theorem implies the parallel repetition of multi-prover games.

4.1.2 Theorem (Verbitsky (1996)). *Let G be a non-trivial multi-prover game with $|Q| = r$ the size of question set. Then,*

$$\operatorname{val}(G^n) \leq \Delta_{r,n}.$$

Applying the theorem of Hillel Furstenberg and Yitzhak Katznelson in (4.1.1), we obtain the following consequence.

4.1.3 Corollary. Let G be a non-trivial multi-prover game. Then, $\lim\limits_{n \longrightarrow \infty} \operatorname{val}(G^n) = 0$.

The theorem (4.1.2) has been proved by Verbitsky (1996) for two-prover games. His proof can be extended for multi-prover games in our case, that is, for k players with $k \geq 2$. To establish the truth of this theorem, Oleg Verbitsky used the proof by contradiction. The general idea is: given a subset W of Q^n, we must show that W is the subset of Q^n without a combinatorial line. [Jan: Say that W is the subset of Q^n for which the provers win for a given strategy.]

So, we assume that there is a combinatorial line and then we show that there is contradiction.

Let us adapt our proof from the proof of Verbitsky (1996) to show the theorem (4.1.2) for multi-prover games, that is, we extend the proof of Oleg Verbitsky from two-prover games to multi-prover games.

Proof. Let G be a $k-$prover game, that is $G(\phi, Q \subseteq X^1 \times \ldots \times X^k, A^1 \times \ldots \times A^k, \mu)$ where X^t and A^t represent respectively the set of questions and the set of answers of the player t, for $1 \leq t \leq k$. The set Q is a subset of the set $X^1 \times \ldots \times X^k$ where elements are chosen randomly according to the probability distribution μ. [Jan: For this proof you have to assume that μ is uniform.]

Let $|Q| = r$, with $Q = \{q_1, \ldots, q_r\}$ where $q_j = (q_j^1, \ldots, q_j^k)$, $q_j^t \in X^t$ for $j \leq r$. The superscript t highlights the component (player), while the subscript j denotes the number (order) of questions. For instance the question q_j^t is the $j-$th question addressed to the player number t. For the parallel repetition G^n, let us consider $F^1, \ldots, F^k$ like the k optimal strategies of the game where each strategy is an $n-$tuple function of strategies, that is $F^t = (f_1^t, \ldots, f_n^t)$. We denote by K the set of success questions using these strategies in G^n. The set K can be expressed as:

$$K = \{(s_1, \ldots, s_n) \in Q^n : \bigwedge_{i=1}^{n} \phi \left[s_i^1, \ldots, s_i^k, f_i^1(s_1^1, \ldots, s_n^1), \ldots, f_i^k(s_1^k, \ldots, s_n^k)\right] = 1\}.$$

[Jan: Before the proof you used W, now you use K. Be consistent.]

Note that for $1 \leq i \leq n$, $s_i \in Q = \{q_1, \ldots, q_r\}$. s_i^t denotes an $i-$th question in parallel repetition addressed to the player t. This question can be any of the $t-$th component of the set q_j.

As K is the set of success questions, then the value of the game G^n is: $\mathrm{val}(G^n) = \frac{|K|}{r^n}$. [Jan: Note that this is the place where you use uniform distribution assumption].

In this stage, we can not say that $\Delta_{r,n} \geq \frac{|K|}{r^n}$ because we do not know if the set K does not contain any combinatorial lines. Let us show that K is a set without a combinatorial line.

Let us suppose by contradiction that there is a combinatorial line $L = \{\bar{b}_1, \ldots, \bar{b}_r\} \subseteq K$. In this case, the game G should be trivial.

Let $C = C_1 \ldots C_n$ be an $r \times n$ matrix whose r rows are $\bar{b}_1, \ldots, \bar{b}_r$ and n columns $C_1 \ldots C_n$ each are either $(q_j, q_j, \ldots, q_j)^T$ for some $j \leq r$ or $(q_1, q_2, \ldots, q_r)^T$. By definition of a combinatorial line, there exists at least one column $C_l = (q_1, q_2, \ldots, q_r)^T$. We assume that L is ordered so that the intersection of the row $\bar{b}_j$ and the column C_l of the matrix is the element q_j. The element $q_j = (q_j^1, \ldots, q_j^k)$ has k components. So, the matrix C can be expanded to the $kr \times n$ matrix D by replacing each matrix element q_j with the column $(q_j^1, \ldots, q_j^k)^T$. There are kr rows of the matrix D and n columns. Thus, let us denote by $\bar{x}_1^1, \ldots, \bar{x}_1^k, \ldots, \bar{x}_r^1, \ldots, \bar{x}_r^k$ the rows of the matrix D where $\bar{x}_j^t \in (X^t)^n$.

Since L is a combinatorial line, let us use one of the strategy of the matrix element in the column C_l which is in the form $(q_1, q_2, \ldots, q_r)^T$. Note that q_j is a $k-$tuple. Let us define strategies

$f^1, f^2, \dots, f^k$ in the game G by $f^t(q^t) = f^t_l(\bar{x}^t_{n_t})$ where $x^t_{n_t} = q^t$ for $1 \leq t \leq k$. These strategies f^t are well defined, since for distinct such n_t and n'_t it holds $\bar{x}^t_{n_t} = \bar{x}^t_{n'_t}$. [Jan: I don't understand last sentence.]

For arbitrary $q_j = (q^1_j, \dots, q^k_j) \in Q$, we have:

$$\phi(q^1, \dots, q^k, f^1(q^1), \dots, f^k(q^k)) = \phi(q^1_j, \dots, q^k_j, f^1_l(\bar{x}^1_j), \dots, f^k_l(\bar{x}^k_j)) = 1$$

As $b_j \in K$, strategies $F^1, \dots, F^k$ win in the $l-$th copy of G. That is the game G is not trivial. [Jan: It *is* trivial.]

Hence, there is a contradiction with our assumption that K contains a combinatorial line.

Therefore, K does not contain a combinatorial line and $\Delta_{r,n} \geq \frac{|K|}{r^n}$. It results that $\mathrm{val}(G^n) \leq \Delta_{r,n}$. □

Let $\nu_{Q,n} = \max_G \mathrm{val}(G^n)$ where the maximum is over all non-trivial games G with set of questions Q. The Oleg Verbitsky's theorem (4.1.2) is applicable to $\nu_{Q,n}$, that is $\nu_{Q,n} \leq \Delta_{r,n}$. [Jan: What is r?] Then, $\lim\limits_{n \longrightarrow \infty} \nu_{Q,n} = 0$.

4.2 Parallel repetition implies Hales-Jewett theorem.

To show that the parallel repetition implies Hales-Jewett theorem, let us firstly define a set of questions on which will be constructed some multi-prover games.

4.2.1 Definition. Let $k \geq 2$ and $Q_k \subseteq \{0,1\}^k$ a question set of size k. An *k-prover question set* is a question set Q_k where the $t-$th question contains 1 in the $t-$th position and 0 in the remaining positions. This question set can be expressed as:

$$Q_k = \left\{ (q^1, \dots, q^k) : |\{t : q^t = 1\}| = 1 \right\}.$$

An extensional definition of the question set Q_k is: $Q_k = \{(1, \dots, 0), (0, 1, \dots, 0), \dots, (0, \dots, 1)\}$. $|Q_k| = k$ and the elements of the question set Q_k are equivalent to the elements of the canonical basis, that is $Q_k = \{e_1, e_2, \dots, e_k\}$ where $e_l = (\delta_{1l}, \delta_{2l}, \dots, \delta_{kl})$, δ_{ml} is the Kronecker delta which equals to 1 if $l = m$ and 0 whenever $l \neq m$ for $1 \leq l, m \leq k$.

Raz theorem can be applied for this question set Q_k. [Jan: It cannot be applied because it is just for two provers.] Let G be a multi-prover game with question set Q_k and $\mathrm{val}(G^{)}$ the value of the $n-$product of G. Then, the question set Q_k admits parallel repetition if $\mathrm{val}(G^n)$ converges to 0 when n converges to infinity. Also, according to Raz theorem, [Jan: Delete "according to Raz theorem".] the question set Q_k admits exponential parallel repetition if there exists $\xi_{Q_k} < 1$ such that for every $n \in \mathbb{N}$:

$$\mathrm{val}(G^n) \leq (\xi_{Q_k})^n.$$

[Jan: This paragraph is not relevant to this section.]

The following theorem highlights that there exists a game such that the parallel repetition of this game implies the density Hales-Jewett theorem. This result announced as theorem (4.2.2) links the existence of a combinatorial line in a set with the parallel repetition value of a certain game.

[Jan: Use \cite* to cite.]

4.2.2 Theorem (Hązła et al. (2016)). *Let $k \geq 3$, $n \geq 1$ and $S \subseteq [k]^n$ with density $\delta = |S|/k^n$ such that S does not contain a combinatorial line.*

There exists a $k-$prover game G_S with question set Q_k and with answer alphabets, $A^t = 2^{[n]} \times [n]$ such that:

- $\mathrm{val}(G_S) \leq 1 - 1/k.$
- $\mathrm{val}(G_S^n) \geq \delta(S).$

Thus, from the theorem (4.2.2) we can deduce the value of the $n-$fold parallel repetition G_S^n when S is the maximum subset of $S \subseteq [k]^n$ without a combinatorial line, that is when the density of S is $\Delta_{k,n} = |S|/k^n$ where $k \geq 3$, $n \geq 1$. This result given as theorem (4.2.3) is complementary to Oleg Verbitsky theorem (4.1.2).

4.2.3 Theorem. *Let $k \geq 3$, $n \geq 1$ and $S \subseteq [k]^n$ with density $\Delta_{k,n}$. We have:* $\mathrm{val}(G_S^n) \geq \Delta_{k,n}$.

For this game G_S, according to the theorems (4.1.2) and (4.2.3), we conclude that $\mathrm{val}(G_S^n) = \Delta_{k,n}$.

To prove the theorem (4.2.2), we need to construct a game which satisfies the conditions on theorem (4.2.2). So, let us construct a game G_S as defined by Hązła et al. (2016) based to the subset S of the set $[k]^n$.

Let $k \geq 3$, $n \geq 1$ and $S \subseteq [k]^n$ with $\delta(S) = \frac{|S|}{k^n}$. The game G_S with question set Q_k which we will define must satisfy the following requirements:

- If S does not contain a combinatorial line, then G_S is non-trivial.
- $\mathrm{val}(G_S^n) \geq \delta(S).$

As $|Q_k| = k$ and $|[k]| = k$, there is a natural bijection between the question tuples in Q_k and $[k]$. So, the game G_S is played as this. The verifier chooses the number of a special prover $t \in [k]$ and sends 1 to the special prover and 0 to all other provers. The answer set of the game G_S is the same for all provers: $A^t = 2^{[n]} \times [n]$ where the power set $2^{[n]}$ denotes the set of all subsets of $[n]$. Note that the set $2^{[n]}$ is equivalent to the set $\{1, 2, \ldots, 2^n\}$. Thus, answers from provers are in the form $(T^1, z^1), \ldots, (T^k, z^k)$. The verifier checks the following conditions and accepts if all of them are met:

- The sets $T^1, T^2, \ldots, T^k$ form a partition of $[n]$.

- $z^1 = z^2 = \ldots = z^k = z$.
- $z \in T^t$
- Let $\bar{s} = (s_1, s_2, \ldots, s_n)$ be the string over $[k]^n$ such that $s_i = e$ if and only if $i \in T^e$ for $1 \leq i \leq n$. Then, $\bar{s} \in S$.

From the definition of the game G_S we can deduce the following propositions given and proved by Hązła et al. (2016). So, the proofs of these propositions are adapted from this latter paper.

4.2.4 Proposition. If S has a combinatorial line, then the game G_S is trivial .

Proof. We assume that $S \subseteq [k]^n$ has a combinatorial line. Let $\bar{b} = w(x) = (b_1, \ldots, b_n)$ an $x-$string for which the combinatorial line is $L(\bar{b}) = \{w(x; i) : i \in [k]\} \subseteq S$ and let fix a position $z \in [n]$ with $b_z = x$. Note that $b_1, \ldots, b_n \in [k] \cup \{x\}$. For $p \in [k] \cup \{x\}$, let us define a set $B(p)$ as: $B(p) = \{j : b_j = p\}$. The set $B(p)$ is the set of coordinates j in which b_j equals to p. Now, let us define the strategy for which prover e will use to answer questions:

$$f^e(q^e) = \begin{cases} (B(e), z) & \text{if } q^e = 0, \\ (B(e) \cup B(x), z) & \text{if } q^e = 1. \end{cases}$$

Thus, the verifier checks the four conditions. The verifier will always accept the first condition because the sets $B(1), \ldots, B(k), B(x)$ from a partition. All z^e are equal, that is $z^1 = \ldots = z^k$, then the second condition is satisfied. Because the prover t responds with $(B(t) \cup B(x), z)$ and $z \in B(x)$, then $z \in T^t$: the third condition is satisfied. The fourth condition is also satisfied because $\bar{s} = \bar{b}$ with t in place of stars and $\bar{s} = \bar{b} = w(t) \in L(\bar{b}) \subseteq S$. □

4.2.5 Proposition. If the game G_S is trivial, then S has a combinatorial line.

Proof. We assume that the game G_S is trivial. So, let $f^1, \ldots, f^k$ be a strategy for the provers that always wins. The form of the answer of the prover e to the question $q \in \{0, 1\}$ is defined as: $(T^e_q, z^e_q) = f^e(q)$ where $e \in [k]$. Since whenever $e \neq t$, the verifier checks $z^e_0 = z^a_1$. As the game is trivial we have $z^1_0 = z^2_0 = \ldots = z^k_0 = z^1_1 = z^2_1 = \ldots = z^k_1 = z$. For any two $e \neq e'$, $T^e_0 \cap T^{e'}_0 = \emptyset$, that the two sets T^e_0 and $T^{e'}_0$ are pairwise disjoint. If $t \neq e$ and $a \neq e'$, the verifier will reject. $z \in T^1_0 \cup \ldots \cup T^k_0$, since if $z \in T^e_0$, the verifier rejects if $t \neq e$. Therefore, the word $\bar{b} = w(x)$ (combinatorial line) is defined as:

$$b_i = \begin{cases} e & \text{if } i \in T^e_0, \text{ for } j \in [k], \\ x & \text{otherwise.} \end{cases}$$

For a fix $t \in [k]$, $w(t) \in S$. We suppose that the verifier picks t as the special prover. Since the verifier checks that the sets T^e form a partition, it must be that prover t responds with $T^t_1 = [n] \ \left(T^1_0 \cup \ldots \cup T^{t-1}_0 \cup T^{t+1}_0 \cup \ldots T^k_0\right)$. The verifier checks that the resulting string is in S and accepts, it must be that $w(t) \in S$. This holds for every t, and thus $L(\bar{b}) \subseteq S$. □

4.2.6 Proposition. The value of G^n_S is at least $\delta(S)$

Proof. Let $T^e = \{i \in [n] : q_i^e = 1\}$. T^e defines the set of coordinates in which prover e is special. In coordinate i, prover e responds with (T^e, i). Let $a_1, \ldots, a_n$ be the sequence of special provers which the verifier picks. Let us assume that if $(a_1, \ldots, a_n) \in S$ then the verifier accepts in all coordinates with probability $\delta(S)$.

Let us show that $\bar{s} = (a_1, \ldots, a_n)$. Since in each coordinate there is exactly one special prover, then the sets $T^1, \ldots, T^k$ form a partition of $[n]$. $z_i^1 = \ldots = z_i^k = i \in T^{t_i}$ by definition of T^e and since prover t_i is pecial in coordinate i. Therefore, $\bar{s} \in S$, since for all n coordinates $\bar{s}$ is exactly the string $(a_1, \ldots, a_n)$. □

[Jan: The language you use in these three propositions cannot be so close to what we have in our paper. You should write these proofs *in your own words*. This means while writing you *should not be looking at my paper*.]

References

Andrew Arana. On the depth of szemerédi's theorem. *Philosophia Mathematica*, 23(2):163–176, 2015.

Boaz Barak, Anup Rao, Ran Raz, Ricky Rosen, and Ronen Shaltiel. Strong parallel repetition theorem for free projection games. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 352–365. Springer, 2009.

Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Anchoring games for parallel repetition. *arXiv preprint arXiv:1509.07466*, 2015.

József Beck. *Combinatorial games: tic-tac-toe theory*, volume 114. Cambridge University Press, 2008.

Michael D Beeler and Patrick E O'neil. Some new van der waerden numbers. *Discrete Mathematics*, 28(2):135–146, 1979.

Felix A Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proceedings of the National Academy of Sciences*, 32(12):331–332, 1946.

Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi 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. ACM, 1988.

Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Efficient identification schemes using two prover interactive proofs. In *Advances in Cryptology—CRYPTO'89 Proceedings*, pages 498–506. Springer, 1990.

Elwyn Ralph Berlekamp. A construction for partitions which avoid long arithmetic progressions. *Canad. Math. Bull*, 11(1968):409–414, 1968.

Thomas F Bloom. A quantitative improvement for roth's theorem on arithmetic progressions. *Journal of the London Mathematical Society*, page jdw010, 2016.

Tom Brown, Bruce M Landman, and Aaron Robertson. Bounds on some van der waerden numbers. *Journal of Combinatorial Theory, Series A*, 115(7):1304–1309, 2008.

Richard Cleve, William Slofstra, Falk Unger, and Sarvagya Upadhyay. Perfect parallel repetition theorem for quantum xor proof systems. In *Computational Complexity, 2007. CCC'07. Twenty-Second Annual IEEE Conference on*, pages 109–114. IEEE, 2007.

Chris Crawford. The art of computer game design. 1984.

Irit Dinur and David Steurer. Analytical approach to parallel repetition. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 624–633. ACM, 2014.

Irit Dinur, Prahladh Harsha, Rakesh Venkat, and Henry Yuen. Multiplayer parallel repetition for expander games. *arXiv preprint arXiv:1610.08349*, 2016.

Pandelis Dodos, Vassilis Kanellopoulos, and Konstantinos Tyros. A simple proof of the density hales–jewett theorem. *International Mathematics Research Notices*, page rnt041, 2013.

Michael R Dransfield, Lengning Liu, Victor W Marek, and Mirosław Truszczyński. Satisfiability and computing van der waerden numbers. *the electronic journal of combinatorics*, 11(1):R41, 2004.

Michael Elkin. An improved construction of progression-free sets. In *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms*, pages 886–905. Society for Industrial and Applied Mathematics, 2010.

Paul Erdos and Richard Rado. Combinatorial theorems on classifications of subsets of a given set. *Proceedings of the London mathematical Society*, 3(1):417–439, 1952.

Paul Erdös and Paul Turán. On some sequences of integers. *Journal of the London Mathematical Society*, s1-11(4):261–264, 1936. ISSN 1469-7750. doi: 10.1112/jlms/s1-11.4.261. URL http://dx.doi.org/10.1112/jlms/s1-11.4.261.

Uriel Feige and László 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. ACM, 1992.

Uriel Feige and Oleg Verbitsky. Error reduction by parallel repetition-a negative result. In *Computational Complexity, 1996. Proceedings., Eleventh Annual IEEE Conference on*, pages 70–76. IEEE, 1996.

Uriel Feige, Guy Kindler, and Ryan O'Donnell. Understanding parallel repetition requires understanding foams. In *Computational Complexity, 2007. CCC'07. Twenty-Second Annual IEEE Conference on*, pages 179–192. IEEE, 2007.

John E Freund. *Introduction to probability*. Courier Corporation, 2012.

Harry Furstenberg. Ergodic behavior of diagonal measures and a theorem of szemerédi on arithmetic progressions. *Journal d'Analyse Mathématique*, 31(1):204–256, 1977.

Hillel Furstenberg and Yitzhak Katznelson. A density version of the hales-jewett theorem. *Journal d'Analyse Mathematique*, 57(1):64–119, 1991.

Hillel Furstenberg, Yitzhak Katznelson, and Donald Ornstein. The ergodic theoretical proof of szemerédi's theorem. *Bulletin of the American Mathematical Society*, 7(3):527–552, 1982.

William Gasarch, Clyde Kruskal, and Andy Parrish. Purely combinatorial proofs of van der waerden-type theorems. *Draft book*, 2010.

W Timothy Gowers. Hypergraph regularity and the multidimensional szemerédi theorem. *Annals of Mathematics*, pages 897–946, 2007.

William T Gowers. A new proof of szemerédi's theorem. *Geometric and functional analysis*, 11 (3):465–588, 2001.

WT Gowers. Fourier analysis and szemerédi's theorem. In *Proceedings of the International Congress of Mathematicians*, volume 1, pages 617–629, 1998.

Ronald L Graham and Bruce L Rothschild. A short proof of van der waerden's theorem on arithmetic progressions. *Proceedings of the American Mathematical Society*, 42(2):385–386, 1974.

Ben Green and Terence Tao. New bounds for szemeredi's theorem, ii: A new bound for r_4 (n). *arXiv preprint math/0610604*, 2006.

Alfred W Hales and Robert I Jewett. Regularity and positional games. *Classic Papers in Combinatorics*, pages 320–327, 1987.

Jan Hązła, Thomas Holenstein, and Anup Rao. Forbidden subgraph bounds for parallel repetition and the density hales-jewett theorem. *arXiv preprint arXiv:1604.05757*, 2016.

Paul R Herwig, Marijn JH Heule, P Martijn van Lambalgen, and Hans van Maaren. A new method to construct lower bounds for van der waerden numbers. *the electronic journal of combinatorics*, 14(1):R6, 2007.

Thomas Holenstein. Parallel repetition: simplifications and the no-signaling case. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 411–419. ACM, 2007.

Michal Kouril and Jerome L Paul. The van der waerden number w (2, 6) is 1132. *Experimental Mathematics*, 17(1):53–61, 2008.

Bundit Laekhanukit. Parameters of two-prover-one-round game and the hardness of connectivity problems. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1626–1643. Society for Industrial and Applied Mathematics, 2014.

Pierre Matet. Shelah's proof of the hales–jewett theorem revisited. *European Journal of Combinatorics*, 28(6):1742–1745, 2007.

Jane McGonigal. *Reality is broken: Why games make us better and how they can change the world*. Penguin, 2011.

Dana Moshkovitz. Parallel repetition from fortification. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 414–423. IEEE, 2014.

Alon Nilli. Shelah's proof of the hales-jewett theorem. In *Mathematics of Ramsey theory*, pages 150–151. Springer, 1990.

Kevin O'Bryant. Sets of integers that do not contain long arithmetic progressions. *the electronic journal of combinatorics*, 18(1):P59, 2011.

DHJ Polymath. A new proof of the density hales-jewett theorem. *arXiv preprint arXiv:0910.3926*, 2009.

DHJ Polymath. Density hales-jewett and moser numbers. *An irregular mind*, pages 689–753, 2010.

DHJ Polymath. A new proof of the density hales-jewett theorem. *Annals of Mathematics*, 175 (3):1283–1327, 2012.

John Rabung and Mark Lotts. Improving the use of cyclic zippers in finding lower bounds for van der waerden numbers. *the electronic journal of combinatorics*, 19(2):P35, 2012.

Robert Alexander Rankin. Xxiv.—sets of integers containing not more than a given number of terms in arithmetical progression. *Proceedings of the Royal Society of Edinburgh. Section A. Mathematical and Physical Sciences*, 65(04):332–344, 1961.

Anup Rao. Parallel repetition in projection games and a concentration bound. *SIAM Journal on Computing*, 40(6):1871–1891, 2011.

Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

Ran Raz. Parallel repetition of two prover games (invited survey). In *Computational Complexity (CCC), 2010 IEEE 25th Annual Conference on*, pages 3–6. IEEE, 2010.

Ran Raz. A counterexample to strong parallel repetition. *SIAM Journal on Computing*, 40(3): 771–777, 2011.

Ran Raz and Ricky Rosen. A strong parallel repetition theorem for projection games on expanders. In *Computational Complexity (CCC), 2012 IEEE 27th Annual Conference on*, pages 247–257. IEEE, 2012.

KF Roth. Irregularities of sequences relative to arithmetic progressions, iii. *Journal of Number Theory*, 2(2):125–142, 1970.

Klaus F Roth. On certain sets of integers. *Journal of the London Mathematical Society*, 1(1): 104–109, 1953.

Saharon Shelah. Primitive recursive bounds for van der waerden numbers. *Journal of the American Mathematical Society*, 1(3):683–697, 1988.

David Steurer. Improved rounding for parallel repeated unique games. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 724–737. Springer, 2010.

RS Stevens and R Shantaram. Computer-generated van der waerden partitions. *Mathematics of Computation*, 32(142):635–636, 1978.

Endre Szemerédi. On sets of integers containing no four elements in arithmetic progression. *Acta Mathematica Academiae Scientiarum Hungarica*, 20(1-2):89–104, 1969.

Endre Szemerédi. On sets of integers containing no k elements in arithmetic progression. *Acta Arith*, 27(199-245):2, 1975.

Suguru Tamaki. Parallel repetition of two-prover one-round games: An exposition. *Interdisciplinary Information Sciences*, 21(4):289–306, 2015.

Terence Tao. A quantitative ergodic theory proof of szemerédi's theorem. *Electron. J. Combin*, 13(1):R99, 2006.

Terence C Tao and Van H Vu. Additive combinatorics. *Bull. Amer. Math. Soc*, 2006.

Bartel Leendert Van der Waerden. Beweis einer baudetschen vermutung. *Nieuw Arch. Wisk*, 15 (2):212–216, 1927.

Oleg Verbitsky. Towards the parallel repetition conjecture. *Theoretical Computer Science*, 157 (2):277–282, 1996.