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

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

2. On the Hales-Jewett theorem

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

2.1 Arithmetic progression

[Jan: This section is OK, but since we don't need infinite arithmetic progressions, I would merge those definitions into one, where you just deal with the finite case.] !

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

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

The arithmetic progression is also known as an arithmetic sequence. The constant is also the difference between 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 $n = 0, 1, \cdots, k-1$, that is k consecutive values of n.

We denote by AP(k) or AP-k, 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 $A_1, A_2, \cdots, A_n$ of mutually nonempty and disjoint subsets of set A (Dransfield et al., 2004). A_i are known as *blocks*. [Jan: This is a common definition, no need for a reference.]

We denote by $\mathbb{Z}^+$, the set of positive integers. Let $m \in Z^+$, we designate by $[m]$ the set $\{1, 2, \cdots, m\}$. [Jan: Use ldots instead of cdots].

Let X be a set and r be a positive integer. We want to colour elements of set X with some 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: For words like r-coloring, write “\$r\$-coloring” instead of “\$r-coloring\$".]

If $|X| = n$, then the number of possibilities of colouring the n elements is n^r.

[Jan: Better: “the number of r-colorings of X is”]

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

[Jan: For restriction better use \restriction and write Y in lower script, like this: $c \restriction_Y$.]

According to Polymath (2009) , 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 $N \in \mathbb{Z}^+$ such that for every $r - colouring$ of [N] there is a monochromatic AP-k.*

[Jan: I think it is more consistent with other theorems to state this as: “there exists N_0 such that for every $N \geq N_0$”]

We know that a $r-$colouring is a function called c in definition (2.2.1). So, in other words there exists $a,\ d\ \in \mathbb{N}$ with $d \neq 0$ such that: $c(a) = c(a + d) = c(a + 2d) = \cdots = c(a + (k - 1)d)$.

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 $N \in \mathbb{Z}^+$ such that for every partition $A_1, \cdots, A_r$ of $[N]$, there is i, $1 \leq i \leq r$, such that block A_i contains an arithmetic progression of least k.*

[Jan: Note that for this version a block in a partition can be empty.]

The existence of the number N for which any $r-$colouring of the integer $\{1, \cdots, N\}$ 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 Van der Waerden (1927).

Graham and Rothschild (1974) gave a 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: G. and R. gave *another* proof of this theorem.]

In this theorem, the difficult problem is to find the number N. The least such number is called *Van der Waerden number* denoted as $W(k,l)$. The general expression of $W(k,l)$ is not known, but for some k and l there are exact values or there are some lower and upper bounds (Dransfield et al., 2004).

[Jan: Be consistent: before you used k and r, now it is k and l.]

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

$W(1,r)=1$: this is an $AP-1$. $W(k,1)=k$: this is an $AP-k$. $W(2,r)=r+1$: this is an $AP-2$. [Jan: Either leave the formulas without explanation or explain better.]

For instance, let us find the Van der Waerden number $W(2,3)$, that is a $2-$colouring of the set $[W(2,3)]$ such that there is a monochromatic arithmetic progression of length 3. [Jan: Shouldn't it be $W(3,2)$?]

The value of $W(2,3)$ is greater than 8 because for any $2-$colouring of $[n]$, $\quad n\in\{3,4,5,6,7,8\}$, we can find a $2-$colouring which does not contain a monochromatic arithmetic progression of length 3. [Jan: Don't use \quad like this, normal space is OK. Maybe give an example for $n=8$?]

So, when $W(2,3)=9$ 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 an form an 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 $\{1,2,\cdots,9\}$

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

$k\setminus r$	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.

As related previously, searching for the exact value of $W(k,r)$ remains a difficult problem to find solution as 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, 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 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 values of Van der Waerden numbers $W(k, r)$.

The estimation of lower and upper bounds is still 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 $W(k, r)$.

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

Berlekamp (1968) found a better bound when $k - 1 =$ prime number and for $r = 2$ (colors). But these bounds still require improvement. [Jan: Do not use symbols inside sentences, write "when $k - 1$ is prime".]

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

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

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

[Jan: Is r above equal to two?]

So, $W(6, 2) > 5 \times 2^5 = 160$, $W(8, 2) > 7 \times 2^7 = 896$ and $W(12, 2) > 11 \times 2^1 1 = 22528$. (Dransfield et al., 2004) improve this lower bound by using propositional satisfiability solvers for some small van der Waerden numbers for instance $W(2, 8) > 1322$. 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). [Jan: W(2, 8) or W(8, 2)?]

The best known upper bound of $W(k, r)$ is the expression (2.3.6) 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:

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

2.3 Szemerédi's theorem

Szemerédi's theorem is merely an extension of Van der Waerden's theorem in terms of *density version*. Below, we show this implication.

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 $0 < \delta \leq 1$.

2.3.1 Theorem (Szemerédi's theorem). *(Polymath, 2009) For every $k \in \mathbb{Z}^+$ and every $0 < \delta \leq 1$ there exists an integer $N(k,\delta) \geq 1$ such that every subset $A \subseteq [N]$ of size $|A| \geq \delta N$ contains an arithmetic progression of length k.*

[Jan: Don't cite Polymath above. Cite nothing or Szemeredi.]

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). 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 all conditions of Szemerédi's theorem (2.3.1) are verified. From Van der Waerden's theorem, let us show that $\forall k, r \in \mathbb{Z}^+, \quad \exists\ N(k,r) \in \mathbb{Z}^+$ such that by $r-$colouring the set $\{1, 2, \cdots, N\}$ (the number $N(k,r)$ depending on k and r), 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. [Jan: Better first sentence: Assume Szemeredi's theorem is true.] [Jan: s/From VDW theorem/To obtain VDW theorem]

Let be a partition of $\{1, \cdots, N\}$ to r blocks, that is $\{1, \cdots, N\} = A_1 \cup A_2 \cup \cdots \cup A_r$, with $A_i \cap A_j \neq 0$. This implies that $A_i \neq \emptyset$. The color of the block A_i is indicated by the number i. There are two blocks with the same colour. [Jan: s/Let be a partition/Partition $[N]$ into r blocks]

Let A_{max} be the set having the largest number of elements. By partitioning $\{1, \cdots, N\}$ to r equal parts, we have: $A_{max} = A_i = \frac{N}{r}$, for $1 \leq i \leq r$. [Jan: I don't get this part.]

If $|A_i| < \frac{N}{r}$, for $1 \leq i \leq r$, then $|A_1| + |A_2| + \cdots + |A_r| < \frac{N}{r} + \cdots + \frac{N}{r} = \frac{rN}{r} = N$, that is $\sum_{i=1}^{r} |A_i| < N$, therefore A_i for $1 \leq i \leq r$ does not form in this case a partition. [Jan: ... which is a contradiction.]

If $|A_i| \leq \frac{N}{r}$, for $1 \leq i \leq r-1$, then $\displaystyle\sum_{i=1}^{r-1} |A_i| \leq \frac{(r-1)N}{r}$. There exists a positive integer a such that $\displaystyle\sum_{i=1}^{r-1} |A_i| = \frac{(r-1)N}{r} - a$. [Jan: How do you know that a is integer? What if A_{max} is not A_r?]

Thus,

$$\begin{aligned} |A_1| + |A_2| + \cdots + |A_r| = N &\iff \frac{(r-1)N}{r} - a + |A_r| = N \\ &\iff |A_r| = \frac{N}{r} + a \end{aligned}$$

Therefore, $|A_r| \geq \frac{N}{r}$. In this case, as $A_{max} = A_r$, then $A_{max} \geq \frac{N}{r}$.

We know that A_{max} is the largest block. Let us assume that $A_{max} = A_r$. It is clear that $|A_{max}| \geq |A_i|$, for $1 \leq i \leq r-1$.

So,

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

$|A_{max}| \geq \frac{N}{r} \iff |A_{max}| \geq \frac{1}{r}N \iff |A_{max}| \geq \delta N$, with $\delta = \frac{1}{r}$, implies according to Szemerédi's theorem (2.3.1) A_{max} contains an arithmetic progression of length k. [Jan: If N is bigger than what?]

Therefore, A_{max} is monochromatic arithmetic progression of length k. [Jan: A_{max} is not a progression.] $\square$

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 equal to the Van der Waerden's number $W(k,r)$ when $\delta = \frac{1}{r}$. [Jan: No, you only know that $W(k,r) \leq N(k,1/r)$.] There is still no a general exact expression of $W(k,r)$, but there are exact values of $W(k,r)$ (7 exact values are known) for some smaller k and r, as far as for the remain cases there are some approximations of the lower and upper bounds of it.

Likewise, for Szemerédi's theorem, the general exact value of $N(k,\delta)$ 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 number.

Before giving quantitative bounds of Szemerédi's theorem existing in the literature, let us formulate differently the Szemerédi's number. Knowing the number $N(k,\delta)$, all subset A of $[N]$ such that $|A| \geq \delta N$ contains an arithmetic progression of length k. Otherwise, we can define the Szemerédi's number as the largest subset of $[N]$ without containing an arithmetic progression of length k. Let us denote by $r_k(N)$ the size of this largest subset. [Jan: This paragraph is not clear, rewrite it.]

Lower bound Behrend (1946) proved that for $k = 3$, $\epsilon > 0$, $C > 0$ an unspecified constant and $\log = \log_2$:

$$r_3(N) \geq \frac{CN}{2^{2\sqrt{2}(1+\epsilon)\sqrt{\log N}}} \tag{2.3.1}$$

[Jan: Don't write $\log = \log_2$, just say that all your logarithms are binary. Is this for every $\epsilon > 0$?]

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

$$r_3(N) \geq \frac{CN(\log N)^{1/4}}{2^{2\sqrt{2}\sqrt{\log N}}} \tag{2.3.2}$$

[Jan: $\sqrt{\log N}$ or $(\log N)^{1/4}$?]

[Jan: Expressions below are very complicated, can you give some explanations or approximations for those numbers?] For $k \geq 1 + 2^{n-1}$, $n = [\log k]$, $\epsilon > 0$, Rankin (1961), cited by O'Bryant (2011) proved that if N is sufficiently large then:

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

Basing on (2.3.1), (2.3.2) and (2.3.3), O'Bryant (2011) constructed the following expressions:

$$r_3(N) \geq N\left(\frac{\sqrt{360}}{e\pi^{3/2}} - \epsilon\right)\frac{\sqrt[4]{2\log N}}{4^{\sqrt{2\log N}}} \tag{2.3.4}$$

$$r_k(N) \geq NC_k 2^{-n2^{(n-1)/2}\sqrt[n]{\log N} + \frac{1}{2n}\log\log N} \tag{2.3.5}$$

where $C_k > 0$ is an unspecified constant. The expression (2.3.5) 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 in this work that the upper bound of $r_k(N)$ is:

$$r_k(N) \leq N(\log\log N)^{-2^{-2^{k+9}}} \tag{2.3.6}$$

where $\delta = (\log\log N)^{-2^{-2^{k+9}}}$. [Jan: What is δ for?]

Bloom (2016) improved the upper bound for $r_3(N)$:

$$r_3(N) \leq C\frac{(\log\log N)^4}{\log N}N. \tag{2.3.7}$$

For $k = 4$, Green and Tao (2006) improved the result (2.3.6) of Gowers (2001) as follows:

$$r_4(N) \leq CNe^{-c\sqrt{\log\log N}} \tag{2.3.8}$$

for some absolute constant $c > 0$.

[Jan: It is usual to write e in normal font, not mathrm.]

Therefore, quantitative bounds of $r_k(N)$ are:

$$NC_k 2^{-n2^{(n-1)/2}\sqrt[n]{\log N}+\frac{1}{2n}\log\log N} \leq r_k(N) \leq N\left(\log\log N\right)^{-2^{-2^{k+9}}} \tag{2.3.9}$$

Quantitative bounds for $k=3$ and $k=4$ have been enhanced. Thus, for $k=4$ we have the equation (2.3.8). By combining (2.3.4) and (2.3.7), we have the quantitative bounds of $r_3(N)$, expressed in (2.3.10)

$$N\left(\frac{\sqrt{360}}{\mathrm{e}\pi^{3/2}}-\epsilon\right)\frac{\sqrt[4]{2\log N}}{4^{\sqrt{2\log N}}} \leq r_3(N) \leq C\frac{(\log\log N)^4}{\log N}N \tag{2.3.10}$$

[Jan: Again, if you insert those bounds, please comment on them. What is the nature of expressions on the left and right? How big is the gap?]

2.4 Hales-Jewett theorem

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

For instance, $k=3$ and $n=6$, an element of the set $[3]^6$ is : 121132.

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

Elements of $([k]\times\{x\})^n$ are called *coordinates*. [Jan: No, coordinate is something else.] x is called *wildcard*.

Given $k, n \in \mathbb{N}$, we call $x-string$ (or $n-$dimensional *variable word* on k letters), a finite word $a_1a_2\cdots a_n$ of the symboles $a_i \in [k]\cup\{x\}$, where at least one symbol a_i is x. $w(x)$ denotes an $x-string$. Let V denote the set of all strings: $V=\{w(x)\}$. The cardinality of V is: $V=(k+1)^n-k^n$.

For any integer $i\in[k]$ and $x-string$ $w(x)$, the string obtained from $w(x)$ by replacing each x by i is denoted by $w(x;i)$. A *combinatorial line* is a set of k strings $\{w(x;i):\ i\in[k]\}$ where $w(x)$ is an $x-string$ (Beck, 2008). That is a combinatorial line is a set of k finite words obtained by replacing x in the word $w(x;i)$ by $i\in\{1,2,\cdots k\}$.

For instance, for $k=3$ and $n=8$, a combinatorial line is :

$\{w(x)=1xx2x23x:\ x\in[3]\}=\{11121231, 12222232, 13323233\}$. [Jan: This is not consistent with your previous notation.]

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

2.4.1 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 bound using simple induction. [Jan: What does primitive recursive mean? When you are writing something, you should be able to explain at least general idea.] Nilli (1990) presented a compact form of Shelah's Proof of the Hales-Jewett Theorem. Matet (2007) presented 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:

2.4.2 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. Polymath (2009) gave an elementary non-ergodic proof of the density version of Hales-Jewett theorem by using the equal-slices measure. A simplified version of Polymath (2009) has been given by Dodos et al. (2013) using a purely combinatorial proof of the density Hales–Jewett Theorem.

To show that this density version of Hales-Jewett implies the Hales-Jewett, 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 (2.4.2), A_{max} contains a combinatorial line.

2.4.3 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 lines corresponds to the arithmetic progression. [Jan: "combinatorial lines correspond to arithmetic progressions".]

In (2.3.2) we have shown that Szemeredi's theorem implies Van der Waerden's theorem. To show that the density version of Hales-Jewett theorem implies Van der Waerden's theorem, we need to show that the density version of Hales-Jewett theorem implies Szemerédi's theorem. Hence, by transitivity, the density version of Hales-Jewett theorem implies Van der Waerden's theorem.

Thereupon, whatever the kind of Hales-Jewett theorem used to establish the implication, we need only to show that the combinatorial line involves the arithmetic progression. [Jan: I'm not sure what you are trying to say here.]

Let us assume that the Hales-Jewett theorem is verified 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 $\{1, 2, \cdots, k\}$. Instead to start by 1, let us start by 0. In this part, $[k]$ expresses the set $\{0, 1, \cdots, k-1\}$. It is obvious that $[k] = \mathbb{Z}/k\mathbb{Z}$.

Let n be the positive number of the Hales-Jewett theorem, then the set $[k]^n = (\mathbb{Z}/k\mathbb{Z})^n = \{(x_0, x_1, \cdots, x_{n-1}) : \ x_i \in [k]\}$ has k^n elements. Similarly, $[k^n] = \{0, 1, \cdots, k^n - 1\}$ has also k^n elements. The set $[k^n]$ contains natural number (in base 10). While, elements of the set $[k]^n$ are the digits in base$-k$ number system of the numbers $\{0, 1, \cdots, k^n - 1\}$.

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

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

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.

The difference between two consecutive elements $w(x; i_1)$ and $w(x; i_2)$ of this combinatorial line is a constant. Let us call this constant $l = (l_0, l_1, \cdots, l_{n-1}) = w(x; i_1) - w(x; i_2)$ with $i_1 > i_2$. [Jan: If they are consecutive, why not call them $w(x; c)$ and $w(x; c+1)$?]

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

$$l_j = \begin{cases} 1 & \text{if } l_j = x \\ 0 & \text{otherwise} \end{cases}$$ [Jan: $l_j = 1$ or $l_j = x$?]

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

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

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 $d = f(l)$. We denote by D the set $\{j : \ l_j = x\}$. d can be expressed as:

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

Thus, $f(w(x; i)) = a + id$, a and d fixed, $0 \leq i \leq k-1$, 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.

We just need to take $N(k, \delta) = k^n$ to establish that the Hales-Jewett theorem implies the Szemerédi's theorem. [Jan: What is n here?] As this latter implies the Van der Waerden's theorem. Similarly, we need to take $N(k, r) = k^n$ to show that the Hales-Jewett theorem implies the Van der Waerden's theorem. [Jan: There is one small additional complication for the density version.]

3. Parallel repetition of multi-prover games.

In this chapter we discuss about the parallel repetition of multi-prover games and we present the connection with the Hales-Jewett theorem. Firstly, notions about multi-prover games are presented. We start to present two-pover games before giving a generalisation. [Jan: add: to multiple provers] These notions are followed by notions about parallel repetition in which we present the theorem that expresses the upper bound of the value of the success probability of the game for the parallel repetition. Finally, the relationship between [Jan: It is important to always say that you mean *density* Hales-Jewett theorem.] Hales-Jewett theorem and the parallel repetition is examined.

3.1 Multi-prover games.

3.1.1 Two-prover games.. 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 $MIP(2,1)$. [Jan: No, MIP is something else (it is a class of languages).] 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 and uniformly by the verifier, that is with a probability distribution measure $\mu : X \times Y \longmapsto \mathbb{R}^+$. [Jan: Is it chosen uniformly or according to μ?] [Jan: Actually, $\mu : Q \to \mathbb{R}^+$.] The verifier sends x to the first prover and y to the second prover. Each prover does not know the question addressed to other and the communication during the games 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 to the pair of questions (x,y) [Jan: s/answer to the pair/answer the pair] 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 of question x [Jan: s/answer of question/answer to question] using the strategy f by prover 1. Whereas $h(y) \in T$ is the answer of 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*" [Jan: Use Latex quotes (open with

", close with "), look at the code to see the difference.] 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, $G = (\phi, Q \subseteq X \times Y, S, T)$ is a game if X, Y, S, T are finite subset and $\phi : Q \times S \times T \longmapsto \{0, 1\}$ is a predicate. That is, a prover game is a $4-$tuple. [Jan: According to your previous discussion μ should also be part of the definition.]

The 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 to each prover.

Let $Pr[\phi(x, y, f(x), h(y)) = 1]$ [Jan: Use \Pr to denote probability in math mode.] be the winning probability associated to the one of the couples (f, h) of the strategies. In this case, the winning probability "*Pr*" can be the expectation is taken to the distribution μ. [Jan: s/expectation is taken to/expectation taken over]

As in all games, the aim of the two players is to maximize the winning probability according to their strategies. Let denote by $\mathrm{val}(G)$ the *value* of the winning probability associated to the optimal strategies of the two provers for the game G. Then, $\mathrm{val}(G)$ is expressed as:

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

[Jan: Indicate over what the probability is taken.]

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

The two-prover game G is called a *free game* if $Q = X \times Y$, that is, questions to players are independent.

The 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. [Jan: Citation for those last definitions would be nice.]

3.1.2 Relationship between graph and two-prover games.. [Jan: s/graph/graphs]

The relationship between graph 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 graph. Some advanced connections are been studied by Laekhanukit (2014); Tamaki (2015); Dinur et al. (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 constraint associated to edge $e \in E$,for example this constraint can be colouring vertices of edge e with different colours chosen in L. [Jan: What is the domain (set) of c_e?]

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 constraints associated to edges. In others words, a two-prover game G consists of a bipartite graph with vertex sets X, Y, an edge set$E \subseteq X \times Y$ and a label set L. [Jan: You are giving a definition that is not equivalent to your previous definition. You should not call two different things with the same name. At the very least you should make clear that this definition is not equivalent to the first one.] !

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:

$$\mathrm{val}(G) = \max_{f,g} \underset{(x,y)\sim E}{\mathrm{P}} \{(f(x), g(y)) \in c_{(x,y)}\}$$

[Jan: Be consistent with probability symbol: either P or Pr everywhere.] ! [Jan: Explain what notation $\mathrm{Pr}_{x,y\sim E}$ means.] !

Let us introduce some elementary notions of *expander graph* which will be useful in the following. Let $X \cup Y$ and $X \times Y$ be respectively the set of vertices and the set of edges of a bipartite graph G. We denote by d_X and d_Y respectively the degree of each vertex $x \in X$ and the degree of each vertex $y \in Y$. [Jan: If set of edges is $X \times Y$, then the graph is complete. Is this what you mean?] ! [Jan: It seems you are assuming that the graph is regular. Say it in the text.] !

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$-|Y|$ [Jan: Proper way to write this in Latex: $|X|$-by-$|Y|$ (the dashes outside math mode).] ! 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 an $|Y|-$by$-|Y|$ unitary matrix 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 $M^*u = \sigma v$. Let us denote by σ_0 the singular value whose absolute value is the largest. As the matrix M is a normalized matrix, then all singular values are between 0 and 1 , therefore the singular value $\sigma_0 = 1$. [Jan: Why is $\sigma_0 = 1$? For which vector is it realized?] ! 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 [Jan: Define first what is (d_X, d_Y)-bipartite graph.] ! with the second singular value $1 - \lambda$. That is the expander graph is based on the notions of a graph, the set of degree of his vertices, and on singular value associated to the normalized adjacency matrix of the graph.

[Jan: Can you give citation for this section?] !

[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.] !

3.1.3 Type 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: Special kind of prover games.

[Jan: Consider deleting this table. In my opinion it is better to explain just one type of game than to write a long list of names without explanations.] !

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). We are dealing with the general case.

Let consider that there are $k-$provers, with $k \geq 2$. So, $k-$tuple of questions $(x_i^1, \cdots, x_i^k) \in_\mu X^1 \times \cdots \times X^k$ (with X^t set of questions) [Jan: What are i and t?] chosen with probability distribution measure μ from a set of question, and $k-$tuple of answers $(a^1, \cdots, a^k) \in A^1 \times \cdots \times A^k$ (with A^t set of answers) according to question $(x^1, \cdots, x^k)$. The distribution measure μ associates an element of $X^1 \times \cdots \times X^k$ to an element of $\mathbb{R}^+ \cap [0, 1]$. [Jan: $\mathbb{R}^+ \cap [0, 1] = (0, 1]$.] 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. We denote by $MIP(k,r)$ the set of properties for which there exists $k-$prover $r-$round games (Ben-Or et al., 1988; Tamaki, 2015). [Jan: This is not correct description of multiple-round games. Please delete this.]

3.2 Parallel repetition.

3.2.1 Parallel repetition for a two-prover games.. Let G be a two-prover games 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 a 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 $G(\phi, Q \subseteq X \times Y, S, T)$ be a game. The product game G^n is the game $G^n(\phi^n, Q^n \subseteq X^n \times Y^n, S^n, T^n)$, 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. Let us express explicitly the sets Q^n and the function 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:

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

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:

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

Where $\bigwedge$ represents the logical connective "AND" (conjunction). [Jan: Very nice explanation so far. You can underline the fact that f_i is a function of $\bar{x}$ and not just x_i.]

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

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 $n-$vectors (answers): $F(\bar{x}) = (f_1(x_1), \ldots, f_n(x_n))$ and $H(\bar{y}) = (h_1(x_1), \ldots, h_n(x_n))$ where $F = (f_1, f_2, \ldots, f_n)$ and $H = (h_1, h_2, \ldots, h_n)$ are strategies with f_i and h_i represent respectively strategies associated to the questions x_i and y_i. [Jan: Now you made mistake: It is not $f_1(x_1)$, but $f_1(\bar{x})$. It is important that you correct it above and below.]

Strategies F and H are functions defined as:

$F : X^n \longrightarrow S^n : \bar{x} \longmapsto F(\bar{x}) = (f_1(x_1), \ldots, f_n(x_n))$ and

$H : Y^n \longrightarrow T^n : \bar{y} \longmapsto F(\bar{y}) = (h_1(y_1), \ldots, h_n(y_n))$.

Now, the winning case occurs when $\bigwedge_{i=1}^{n} \phi[x_i, y_i, f_i(\bar{x}), h_i(\bar{y})] = 1$, 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:

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

Let us notice that the game G^n can be defined inductively as $G^1 = G, G^2 = G \times G, \ldots, G^n = G \times G^{n-1}$. [Jan: You never introduce what is the product of two games. Better delete this.]

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, $\mathrm{val}(G) = \max_{f,g} Pr[\phi(x, y, f(x), h(y)) = 1]$.

  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: $F = (f_1, \ldots, f_n)$ and $H = (h_1, \ldots, h_n)$. 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 independently and uniformly according to a distribution of probability, then the winning probability becomes:

  $Pr\left[\bigwedge_{i=1}^{n} \phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1\right] = \prod_{i=1}^{n} Pr\left[\phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1\right]$. [Jan: Be careful, this equation is true only for your special strategies, not in general.]

  [Jan: Better put those equations in extended math mode ($$).]

  Let us chose the optimal strategies f and h of G to play each parallel copy of G, that is $f_i = f$ and $h_i = h$ for $1 \leq i \leq n$. Then, the success probability becomes: [Jan: No, f_i is function of $\bar{x}$ and f function of x_i. This is important!]

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

  (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:

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

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

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

Proof.

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

[Jan: The second equation above is not true.] [Jan: In the equations above, indicate over what the probability is taken.] Hence, $\mathrm{val}(G^n) \leq \mathrm{val}(G)$. □

[Jan: I think it is very important that you give some examples illustrating the problem. Try finding a simple game G such that $\mathrm{val}(G^2) > \mathrm{val}(G)^2$.]

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. The history of the theory on parallel repetition of prover games is not old than the history of set theory. [Jan: Delete previous sentence.] 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 say that a set Q of questions admits *exponential parallel repetition* if there exists $\xi_Q < 1$ such that for every $n \in \mathbb{N}$:

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

[Jan: This paragraph does not belong here.]

We denote by $|S|$ and $|T|$ respectively the size of the sets of answers S and T of the game G. The size of the game G is $|S||T|$. [Jan: No, size of the game is usually something else. Delete this.] 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 size answer. 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 smaller ($x \longrightarrow 0$): $1 + x = e^x$, [Jan: Write it differently: you can say that for x close to 0: $1+x \approx e^x$, or, more precisely, $e^x = 1+x+O(x^2)$.] the bound of $\mathrm{val}(G^n)$ as expressed in (3.2.3) can be rewritten as follows:

$\mathrm{val}(G^n) \le (1-\epsilon^c)^{\Omega(n/s)} \le \left(e^{-\epsilon^c}\right)^{\Omega(n/s)} = \exp(-\epsilon^c \Omega(n/s))$. Then, $\mathrm{val}(G^n) \le \exp(-\epsilon^c \Omega(n/s))$.

Or $\mathrm{val}(G^n) \le \exp(-\epsilon^c \Omega(n/s)) = \exp(\frac{-\epsilon}{2} 2\epsilon^{c-1}\Omega(n/s)) = \exp(\frac{-\epsilon}{2})^{2\epsilon^{c-1}\Omega(n/s)} = (1-\frac{\epsilon}{2})^{2\epsilon^{c-1}\Omega(n/s)}$. Then, $\mathrm{val}(G^n) \le (1-\epsilon/2)^{2\epsilon^{c-1}\Omega(n/s)}$. [Jan: Something is confused here. Why ϵ^{c-1}? You should use $\exp(-\epsilon/2) \le (1-\epsilon)$ (for what ϵ?), where is it?]

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: $\mathrm{val}(G^n) \le \left(1 - \frac{(1-\mathrm{val}(G))^3}{6000}\right)^{\frac{n}{\log(|A||B|)}}$. 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[1], [Jan: You don't need this footnote, since you defined projection games before. Also, the definition in the footnote is not the same as in the text.] Rao (2011) improved the bound of this game by finding $c = 2$ and by expressing the function Ω without s. This bound is: $(1-\epsilon^2)^{\Omega(n)}$. 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 the value of the repeated game is bounded as follows:

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

for general games and if the game is the projection game, then the value of the game is:

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

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

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, [Jan: s/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 $n \ge \Omega(m^2)$, the value of the parallel repetition (n times) of this odd cycle game is at least $1-(1/4m^2)^{O(n)}$. [Jan: I don't understand how you computed this.] That is, the lower bound value of parallel repetition of two-prover games is at least $(1-\epsilon^2)^{\Omega(n/s)}$ and can not reach $(1-\epsilon)^{\Omega(n/s)}$.

A projection game, a unique game, and a XOR game are kinds of odd cycle games. [Jan: The other way around: odd cycle game is a special projection game etc.] Hence, they do not have a

[1] In a projection game, for any two questions x and y to the players and any answer β of player 2, there exists at most one acceptable answer α for player 1.

strong parallel repetition. Contrary to others works [Jan: What works? I think you misunderstood something. I'm sure there is no contradiction in literature.] having proved that a strong parallel repetition for these theorems exists, the work of Raz (2011) shows a need of rethinking these works so that the views on the existence or not of strong parallel repetition of two-prover games converge.

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 $\mathrm{val}(G) \leq \rho$, then

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

Dinur and Steurer (2014) establishes that this value (3.2.3) of a $n-$ fold parallel repetition of projection games G and the one of Rao (2011) [Jan: Which bound by Rao? Give equation number.] with improved bounds 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.

We are mainly interested by the upper bound of the value of the parallel repetition. Even if there is no a great interest to the lower bound, [Jan: I think lower bounds are very interesting!] there exists some works which approximate the lower bound. 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
$(1-\epsilon^3 3)^{\Omega(n/s)}$	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, $n \geq \Omega(m^2)$	Raz (2011)
$1-O(\sqrt{\epsilon n s})$	Unique	Steurer (2010)

Table 3.2: Summary of known bounds

3.2.4 Parallel repetition of mutli-prover games. Let $G(\phi, X^1 \times X^k, A^1, \ldots, A^k)$ 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. [Jan: What happened to Q?]

The $n-$fold parallel repetition of the game G is the $k-$prover game $G^n(\phi^n, (X^1)^n \times \ldots \times (X^k)^n, (A^1)^n, \ldots, (A^k)^n)$, 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 superscript $1 \leq t \leq k$ 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). $((x_1^1, \cdots, x_1^k), (x_2^1, \cdots, x_2^k), \ldots, (x_n^1, \cdots, x_n^k)) \in_{\mu^n} Q^n$ 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 and uniformly 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 Q^n. [Jan: Belongs to Q^n? I think it is $(X^t)^n$.] So, 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:

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

[Jan: No! $f_i^t : (X^t)^n \to A^t$]

Thus, the value of the parallel repetition of the multi-prover game G denoted by $val(G^n)$ 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[2] 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 H_G, a spectral gap of the Laplacian [Jan: Laplacian? This is not consistent with your previous description of expanders.] of the graph H_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 $\Omega(n/s) = \frac{c\lambda^2 n}{\log|A|}$. [Jan: This is assuming λ is constant!]

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 section, we present the connection between Hales-Jewett theorem and the parallel repetition of multi-prover games.

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

3.3 Connection with Hales-Jewett theorem.

In both versions of Hales-Jewett theorem (see (2.4.1) and (2.4.2)), 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 (**??**), we have already explain deeply and define what the combinatorial is. Let us recall some outlines of 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 $w(x) = a_1 a_2 \ldots a_n \in ([k] \times \{x\})^n \setminus [k]^n$. That is, in $w(x) = a_1 a_2 \ldots a_n$, 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.

So, the *combinatorial line* is the set of k strings $\{w(x; i) : \; i \in \{1, 2, \ldots, k\}\}$, that is the set $\{w(x; 1), w(x; 2), \ldots, w(x; k)\}$. A combinatorial line can also be written as a $k \times n$ matrix where the lines are formed by $w(x; i)$ for $i \in \{1, 2, \ldots, k\}$ and columns are formed either by a_i that is $(a_i a_i \ldots a_i)^T$ for some $i \in [k]$ or by $(12 \ldots k)^T$ (T denotes transpose).

So, the Hales-Jewett theorem states that for any pair of positive integers k and r, there exists a large enough number n (depending on k and r) such that any $r-$colouring of the set $[k]^n$ contains a monochromatic combinatorial line.

For 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 $\delta = \delta(A)$.

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. [Jan: It is not necessary to repeat concepts from the previous chapter in such detailed way.] !

We denote by $\Delta_{k,n}$ the maximum density of a subset W of $[k]^n$ without a combinatorial line.

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.

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

[Jan: Be clear that this *is* the density Hales-Jewett theorem! Hales-Jewett was proved by Hales and Jewett and the density version (density Hales-Jewett) was proved by Furstenberg and Katznelson.] !

This theorem states that for $k \geq 2$, the maximum density of a subset of $[k]^n$ converges to 0 when n converges to infinity.

The proof of this theorem has been given by Furstenberg and Katznelson (1991) without explicit bounds. Polymath (2012) give 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 has been 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.] ‘

The theorem (3.3.1) implies the Raz theorem (3.2.3). [Jan: No, it does not. The bounds from theorem by Raz are not comparable to those ones.] The Raz theorem (3.2.3) has been conjectured by Feige and Lovász (1992) and demonstrated by Raz (1998). This conjecture stipulates that the value of a parallel repetition of a game (non trivial) decreases exponentially fast to 0 when n converges to infinity. This implication is shown in the following part as a consequence of the Oleg Verbitsky theorem in (3.3.2).

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

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

Applying the theorem of Hillel Furstenberg and Yitzhak Katznelson in (3.3.1), we obtain the following consequence.

3.3.3 Corollary. Let G be a nontrivial multi-prover game. Then, $\lim\limits_{n \longrightarrow \infty} \mathrm{val}(G^n) = 0$.

Before proving the theorem (3.3.2), the following propositions are useful to understand the proof of this latter. [Jan: These propositions are relevant only to the other direction. Please prove Verbitsky's theorem directly here.]

Let r and n be two positive numbers, $S \subseteq [r]^n$ with density $\delta = \frac{|S|}{r^n}$. Let G be a $r-$prover question set with cardinal of the question set Q equals to $[r]$, that is $|Q| = [r]$. We denote by G_S the game with question set Q. A more explanation about G_S is given in the following part.

3.3.4 Proposition (Hązła et al. (2016)). S has a combinatorial line if and only if the game G_S is trivial

[Jan: You have to define G_S before stating the proposition.]

It is clear that in this proposition there are two implications. Thus, the proof of these two implications, hence of the proposition has been given by Hązła et al. (2016). The proof is based on the partition of the set $[n]$ into r sets: $T^1, \ldots, T^r$ whereupon sampling a special prover a and receiving answers $(T^1, z^1), \ldots, (T^r, z^r)$ with $z^j \in [n]$ for $1 \leq j \leq r$.

The following conditions checked and accepted by the verifier if all of them are met, highlight the link between G and S denoted by G_S:

- The sets $T^1, T^2, \ldots, T^r$ form a partition of $[n]$.
- $z^1 = z^2 = \ldots = z^r = z$.
- $z \in T^a$.
- Let $s = (s_1, s_2, \ldots, s_n)$ be the string over $[r]^n$ such that s $i = j$ if and only if $i \in T^j$. Then, $s \in S$.

3.3.5 Proposition (Hązła et al. (2016)). The value of G_S^n is at least $\delta(S)$

The value of the game G_S^n is lower bounded by the density of S. Likewise, Hązła et al. (2016) gave the proof of this proposition based on the partition of the set $[n]$ as defined previously.

Now, we have all the necessary to show the theorem (3.3.2). This theorem has been proved by Verbitsky (1996) using a two-prover games. His proof can be extended for multi-prover games 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 maximum subset of Q^n without a combinatorial line. [Jan: Not necessarily maximum.] So, we assume that there is a combinatorial line and then we show that there is contradiction.

Let us adapt the proof of Verbitsky (1996) to show the theorem (3.3.2) for multi-prover games, that is to extend the proof of Oleg Verbitsky from two-prover games to multi-prover games.

Proof. Let G be a $k-$prover game, that is $G(\phi, Q \subseteq X^1 \times \ldots \times X^k, A^1 \times \ldots \times A^k)$ 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 $X^1 \times \ldots \times X^k$ chosen randomly and uniformly according to a probability distribution. [Jan: Q is chosen randomly? This is not correct.] 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 $F^1, \ldots, F^k$ are the optimal strategies of the game where each strategy is a $n-$tuple function of strategies, that is $F^t = (f_1^t, \ldots, f_n^t)$. We denote by W the set of success questions using these strategies in G^n. The set W can be expressed as:

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

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 W is the set of success questions, then the value of the game G^n is: $\mathrm{val}(G^n) = \frac{|W|}{r^n}$.

In this stage, we can not say that $\Delta_{r,n} = \frac{|W|}{r^n}$ [Jan: Not equal, it should be $\geq$.] because we do not know if the set W does not contain any combinatorial lines. Let us show that W is a set without a combinatorial line.

Let us suppose by contradiction that there is a combinatorial line $L = \{\bar{b}_1, \ldots, \bar{b}_r\} \subseteq W$. In this case, according to the proposition (3.3.4) let us show that the game G should be trivial. [Jan: Game G has nothing to do with the proposition.]

Let $C = C_1 \ldots C_n$ be a $r \times n$ 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 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 $f^1, f^2, \ldots, f^k$ in the game G by $f^t(q^t) = f_l^t(\bar{x}_{n_t}^t)$ where $x_{n_t}^t = q^t$ for $1 \leq t \leq k$. These strategies f^t are well defined, since for distinct such n_t and n_t' it holds $\bar{x}_{n_t}^t = \bar{x}_{n_t'}^t$.

For arbitrary $q_j = (q_j^1, \ldots, q_j^k) \in Q$, we have:

$$\phi(q^1, \ldots, q^k, f^1(q^1), \ldots, f^k(q^k)) = \phi(q_j^1, \ldots, q_j^k, f_l^1(\bar{x}_j^1), \ldots, f_l^k(\bar{x}_j^k)) = 1$$

As $b_j \in W$ and strategies $F^1, \ldots, F^k$ win 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 W contains a combinatorial line.

Therefore, W does not contain a combinatorial line and $\Delta_{r,n} = \frac{|W|}{r^n}$. [Jan: Change $=$ to $\leq$.] It results that $\mathrm{val}(G^n) \leq \Delta_{r,n}$. □

3.3.6 Forbidden subgraph bounds. Let n be a positive integer, G a prover game. A forbidden subgraph bound is a method which attempts to bound $\mathrm{val}(G^n)$ only as a function of X^t, Q, μ, $\mathrm{val}(G)$ and n, and ignores the predicate ϕ and the answers set A^t for $1 \leq t \leq k$. In this section, we present some results about the connection between Hales-Jewett theorem and forbidden subgraph bounds, but mainly for upper bounds of $\mathrm{val}(G)$ that depend only on the questions set Q and n. Feige and Verbitsky (1996) give a further explanation about the forbidden subgraph.

Let $\nu_{Q,n} = \max_G \mathrm{val}(G^n)$ where the maximum is over all non-trivial games G with question set Q.

The theorem in (3.3.2) is applicable to $\nu_{Q,n}$, that is $\nu_{Q,n} \leq \Delta_{r,n}$. Then, $\lim\limits_{n \longrightarrow \infty} \nu_{Q,n} = 0$. [Jan: Delete stuff about forbidden subgraph bounds, you don't have space for that.]

For further result, let us define a question set Q on which a multi-prover game G is constructed.

3.3.7 Definition. Let $k \geq 2$ and $Q_k \in \{0,1\}^k$ 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:

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

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

The following results link the existence of the parallel repetition value of a certain game with or without a combinatorial line in a set.

3.3.8 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:

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

The power set $2^{[n]}$ denotes the set of all subsets of $[n]$. The set $2^{[n]}$ is equivalent to the set $\{1, 2, \dots, 2^n\}$.

A short proof of the theorem (3.3.8) has been given by Hązła et al. (2016) by using the proposition (3.3.10) and theorem (3.3.9) which contain the notion of *homomorphism* of question sets. Let us introduce notions of homomorphism.

Let $k \geq 2$ and $Q \subseteq X^1 \times \ldots \times X^k$ be a $k-$prover question set. Consider the $r-$regular, $r-$partite hypergraph[3] $G = (X^1 \times \ldots \times X^k, Q)$.

Given two hypergraphs $(X^1 \times \ldots \times X^k, Q)$ and $(Y^1 \times \ldots \times Y^k, P)$. The function $f = (f^1, \dots, f^k)$ where $f^t : X^t \longrightarrow Y^t$ is a homomorphism from Q to P if $\bar{q} = (q^1, \dots, q^k) \in Q$ implies $f(\bar{q}) = (f^1(q^1), \dots, f^k(q^k)) \in P$.

Let $S \subseteq Q^n$ with $\delta(S) = |S|/|Q^n|$ the density of S, and $f = (f_1, \dots, f_n)$ be a vector of n homomorphisms of Q (from Q to Q). f is *good* for S if:

- For every $\bar{q} = (q^1, \dots, q^k) \in Q$, we have $f(\bar{q}) = (f_1(\bar{q}), \dots, f_n(\bar{q})) \in S$.
- There exists $i \in [n]$ such that f_i is identity.

[Jan: Please summarize the direct proof, not the one with homomorphisms.] !

3.3.9 Theorem (Feige and Verbitsky (1996)). *Let Q be a connected, $k-$prover question set and $S \subseteq Q^n$. There exists an $k-$prover game G_S with question set Q such that:*

- *If G^S is trivial, then there exists a homomorphism vector f that is good for S.*
- $\operatorname{val}(G_S^n) \geq \delta$.

3.3.10 Proposition. Let $r \geq 3$ and $S \subseteq Q_k^n \cong [r]^n$ such that there exists a homomorphism vector f that is good for S. Then, S contains a combinatorial line.

[3] A hypergraph is pair (X, E) where X is a set of elements called *nodes* or *vertices*, and E is a set of non-empty subsets of X called hyperedges (set of nodes) or edges. For further reading, see https://en.wikipedia.org/wiki/Hypergraph

Moreover, let us consider that S is a subset of $[k]^n$ without a combinatorial line. Assume that S is the maximum subset of $[k]^n$ without a combinatorial line, then from theorem (3.3.8) we obtain the theorem (3.3.11) which is a complementary inequality to theorem (3.3.2).

3.3.11 Theorem (Hązła et al. (2016)). *For $k \geq 3$, $\Delta_{k,n} \leq \mathrm{val}(G^n)$.*

Considering that $\nu_{Q,n} = \max_G \mathrm{val}(G^n)$ where the maximum is over all non-trivial games G with question set Q, we have $\Delta_{k,n} \leq \nu_{Q,n}$ which remains true.

By combining the two theorems (3.3.2) and (3.3.11), we have $\mathrm{val}(G^n) = \Delta_{k,n}$.. Likewise, the maximum value of all non-trivial games equals to the density of the maximum subset of $[k]^n$ without a combinatorial line, that is $\nu_{Q,n} = \Delta_{k,n}$.

From the best known lower bound of $\Delta_{k,n}$ established by Polymath (2010), we can apply it to bound $\mathrm{val}(G^n)$. This lower bound adapted by Hązła et al. (2016), thereafter for this kind of multi-prover is formulated in (3.3.12)

3.3.12 Theorem. *Let $\ell \geq 1$ and $k = 2^{\ell-1} + 1$. There exists $C_\ell > 0$ such that for every $n \geq 2$ there exists a set $S \subseteq [k]^n$ with*

$$\delta(S) \geq \exp\left(-C_\ell (\log n)^{1/\ell}\right)$$

such that S does not contain a combinatorial line

As $\mathrm{val}(G_S^n) \geq \delta(S)$, we deduce from (3.3.12) that $\mathrm{val}(G_S^n) \geq \exp\left(-C_\ell (\log n)^{1/\ell}\right)$ for $k = 2^{\ell-1} + 1$.

[Jan: The section with proofs seems disorganized. Please divide it clearly into two parts (DHJ => PR) and (PR => DHJ) without mixing them up.] !

References

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.

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.

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.

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.

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.