The independence number of the orthogonality graph in dimension $2^k$

Hajime Tanaka
(joint work with Ferdinand Ihringer)
Research Center for Pure and Applied Mathematics
Graduate School of Information Sciences
Tohoku University

September 28, 2019
Frontiers in Mathematical Science Research Workshop
About myself

Research area:
- algebraic combinatorics
- algebraic graph theory
- spectral graph theory

Professional background
- Mar ’04 : Ph.D. in Math from Kyushu U
- Apr ’04 – Mar ’07 : JSPS postdoc at GSIS, Tohoku U
- Apr ’07 – Sep ’07 : in USA (WPI, MIT)
- Oct ’07 – Jul ’12 : Assist. Prof. at GSIS, Tohoku U
- Aug ’12 – : Assoc. Prof. at GSIS, Tohoku U
- Apr ’17 – : Assoc. Prof. at RACMaS, Tohoku U
Pseudo-telepathy game
(Brassard–Cleve–Tapp (’99))

Alice & Bob have no communication after the game starts.

They receive $n$-bit strings (questions)

$$x = (x_1, \ldots, x_n), \; y = (y_1, \ldots, y_n) \in \{0,1\}^n$$

where $n = 2^k$, such that

$$\partial(x, y) = 0 \text{ or } n/2.$$

They respond with $s$-bit strings (answers)

$$a = (a_1, \ldots, a_s), \; b = (b_1, \ldots, b_s) \in \{0,1\}^s.$$

They win if $x = y \iff a = b$. 
Theorem (Brassard–Cleve–Tapp). The pseudo-telepathy game can be won with

\[ s = k = \log_2 n, \]

if Alice & Bob are allowed to use \( k \)-qubit quantum systems in the maximally entangled state.

Question. How small can \( s \) be to win the classical pseudo-telepathy game?
The orthogonality graph $\Omega_n (n = 2^k)$

- $V = V(\Omega_n) = \{0,1\}^n$ (vertex set)
- $E = E(\Omega_n) = \{\{x, y\} : x, y \in V, \partial(x, y) = n/2\}$ (edge set)
Coloring of $\Omega_n$

Alice & Bob receive $x, y \in V = \{0,1\}^n$ such that
\[ \partial(x, y) = 0 \text{ or } n/2. \]

They respond with $a, b \in \{0,1\}^s$ so that
\[ x = y \iff a = b. \]

Alice & Bob’s answers are functions $f : x \mapsto a$, $g : y \mapsto b$.

We must have $f = g$.

Moreover, we also have
\[ \partial(x, y) = n/2 \implies f(x) \neq f(y). \]

\[ x \quad - \quad \bullet \quad y \]
Coloring of $\Omega_n$

- The function $f : V \rightarrow \{0,1\}^s$ satisfies
  \[ x \neq y \implies f(x) \neq f(y). \]
  \[ f : V \rightarrow \{0,1\}^s \]
  \[ x \sim y \implies f(x) \neq f(y). \]
  \[ x \text{ is "colored" by } a \]

- In other words, for every $a \in \{0,1\}^s$, the set
  \[ f^{-1}(a) = \{ x \in V : f(x) = a \} \]
  is an independent set, i.e., no two vertices are adjacent.

- Moreover, these sets partition the vertex set $V$:
  \[ V = \bigsqcup_{a \in \{0,1\}^s} f^{-1}(a). \]

- Thus, $\Omega_n$ has a coloring with $2^s$ colors.
The chromatic number of $\Omega_n$

- The chromatic number $\chi(\Omega_n)$ of $\Omega_n$ is the smallest number of colors in a coloring of $\Omega_n$.

**Remark.** We can show $\chi(\Omega_n) \geq n = 2^k$ in general.

**Summary.**

- Alice & Bob win the classical pseudo-telepathy game
  \[\iff \Omega_n \text{ has a coloring with } 2^s \text{ colors} \iff s \geq \log_2 \chi(\Omega_n) \geq k\]

- Alice & Bob win the quantum pseudo-telepathy game with $s = k$. Estimate the gap!!
The independence number of $\Omega_n$

**Problem.** Estimate $\log_2 \chi(\Omega_n) \ (\geq k)$.

**Theorem** (Galliard (’01), Godsil–Newman (’08)).

$$\log_2 \chi(\Omega_n) = k \iff k \in \{1, 2, 3\} \ (\text{i.e., } n \in \{2, 4, 8\}).$$

The independence number $\alpha(\Omega_n)$ of $\Omega_n$ is the largest size of an independent set of $\Omega_n$.

**Lemma.** $\chi(\Omega_n) \alpha(\Omega_n) \geq |V| = 2^n = 2^{2^k}$.

**Proof.** A coloring is a partition of $V$ into independent sets. ■
The main problem of this talk

Lemma. $\chi(\Omega_n) \alpha(\Omega_n) \geq |V| = 2^n \left( = 2^{2^k} \right)$. 

Corollary. $\chi(\Omega_n) \geq 2^n / \alpha(\Omega_n)$. 

Problem'. Find $\alpha(\Omega_n)$, the independence number of $\Omega_n$. 
The main problem of this talk

Problem’. Find $\alpha(\Omega_n)$, the independence number of $\Omega_n$.

Galliard (’01) found an independent set of $\Omega_n$ of size

$$4 \sum_{i=0}^{n/4-1} \binom{n-1}{i},$$

and conjectured that this equals $\alpha(\Omega_n)$ for all $n = 2^k$.

De Klerk & Pasechnik (’07) proved this for $n = 16 = 2^4$, i.e., $\alpha(\Omega_{16}) = 2304$, using the semidefinite programming bound due to Schrijver (’05) based on the Terwilliger algebra.

This gives $\chi(\Omega_{16}) \geq 2^{16}/2304 = 2^{4.83}$.

We need extra .83 bit!!
The main result

**Theorem** (Ihringer–T. ('19)). For all $n = 2^k$ ($k \geq 2$), we have

$$\alpha(\Omega_n) = 4 \sum_{i=0}^{n/4-1} \binom{n-1}{i}.$$ 

The proof is a modification of Frankl’s *rank argument* ('86).

The proof is just around one page, assuming a bit of knowledge on association schemes.

I will explain what I think is most interesting in this proof.
A proof sketch

By Galliard’s construction, we know

\[ \alpha(\Omega_n) \geq 4 \sum_{i=0}^{n/4-1} \binom{n-1}{i}. \]

Hence it suffices to show that \( \text{LHS} \leq \text{RHS} \).

Then the proof is reduced to showing the following:
A proof sketch

Claim. The matrix

\[
\left( \varphi(\partial(x, y)) \right)_{x, y \in C}
\]

is non-singular for any \( C \subset \{0,1\}^{n-1} \) such that

\[
\{ \partial(x, y) : x, y \in C \} \subset \{2i : 0 \leq i < n/2, i \neq n/4\},
\]

where

\[
\varphi(\xi) = \binom{\xi/2 - 1}{n/4 - 1} = \frac{(\xi/2 - 1)(\xi/2 - 2)\cdots(\xi/2 - n/4 + 1)}{(n/4 - 1)!}.
\]

degree \( n/4 - 1 \)
Indeed, from every independent set in $\Omega_n$ we can construct four such $C$’s, and we have

$$|C| = \operatorname{rank} \left( \varphi(\partial(x, y)) \right)_{x, y \in C} \leq \operatorname{rank} \left( \varphi(\partial(x, y)) \right)_{x, y \in \{0,1\}^{n-1}} \leq \sum_{i=0}^{n/4-1} \binom{n-1}{i},$$

follows from Claim

where the last $\leq$ uses association scheme theory.
A proof sketch

Recall the matrix

\[
\begin{pmatrix}
\varphi(\partial(x, y))
\end{pmatrix}_{x, y \in C},
\]

where

\[
\{ \partial(x, y) : x, y \in C \} \subset \{ 2i : 0 \leq i < n/2, \ i \neq n/4 \},
\]

and

\[
\varphi(\xi) = \begin{pmatrix}
\frac{\xi}{2} - 1 \\
\frac{n}{4} - 1
\end{pmatrix} = \frac{(\xi/2 - 1)(\xi/2 - 2)\cdots(\xi/2 - n/4 + 1)}{(n/4 - 1)!}.
\]
A proof sketch

Recall the following result:

**Theorem (Lucas).** Let \( p \) be a prime, and let

\[
a = \sum_{j=0}^{r} a_j p^j, \quad b = \sum_{j=0}^{r} b_j p^j
\]

be \( p \)-adic expansions of non-negative integers \( a \) and \( b \). Then

\[
\binom{a}{b} \equiv \prod_{j=0}^{r} \binom{a_j}{b_j} \pmod{p}.
\]

\( \binom{\alpha}{\beta} := 0 \) if \( \alpha < \beta \)

\[
a = a_r a_{r-1} \cdots a_1 a_0 \pmod{p}
\]

\[
b = b_r b_{r-1} \cdots b_1 b_0 \pmod{p}
\]
A proof sketch

As \( n/4 - 1 = 2^{k-2} - 1 = \sum_{j=0}^{k-3} 2^j \), we have

\[
\binom{i-1}{n/4 - 1} \equiv 0 \pmod{2} \quad (0 < i < n/2, i \neq n/4).
\]

\[
i - 1 = a_{k-2} a_{k-3} \ldots a_1 a_0 \quad (2)
\]

\[
n/4 - 1 = 0 \ 1 \ \ldots \ 1 \ 1 \quad (2)
\]

Hence \( \left( \varphi(\partial(x, y)) \right)_{x,y \in C} \equiv I \pmod{2} \)

\[\blacksquare\]