**Corrections**

**BIOPHYSICS AND COMPUTATIONAL BIOLOGY**

The authors note that the second sentence in the Acknowledgments, “This work was supported by National Institutes of Health (NIH) Grants GM059273 (to A.G.P.) and GM062270 (to L.S.)” should instead appear as “This work was supported by National Institutes of Health (NIH) Grants GM059273 (to A.G.P.) and GM062270 (to L.S.) and by National Science Foundation Grant MCB-0918535 (to B.H.).”

**DEVELOPMENTAL BIOLOGY**

The authors note that, due to a printer’s error, refs. 33–38 were numbered incorrectly. The citations to the reference numbers are correct in the text. Below is the correct order for refs. 33–38.


**IMMUNOLOGY**

The authors note that the author name Jin Tengchuan should instead appear as Tengchuan Jin. The corrected author line appears below. The online and print versions have been corrected.


**MATHEMATICS**

The authors note that, due to a printer’s error, on page 19227, left column, first full paragraph, line 6 “Gn” should instead appear as “a ∈ R”. Also, on page 19227, left column, first full paragraph, line 7 “x ∈ V(Hn)” should instead appear as “x ∈ S”. Both the online article and the print article have been corrected.

www.pnas.org/cgi/doi/10.1073/pnas.1301191110

www.pnas.org/cgi/doi/10.1073/pnas.1301191110

The authors note that the following statement should be added as a Note Added in Proof: “Estimates of the occurrence of Earth analog planets appear in several previous works including Catanzarite and Shao (25), Traub (26), and Dong and Zhu (27). These estimates, which range from 1% to 34%, were built upon early catalogs of Kepler planet candidates (based on less than 1.3 years of photometry). These estimates did not address survey completeness with injection and recovery or uncertain stellar radii with spectroscopy.” The online version has been updated to include the following three references:


www.pnas.org/cgi/doi/10.1073/pnas.1321363110
Violating the Shannon capacity of metric graphs with entanglement

Jop Briët\textsuperscript{a,1}, Harry Buhrman\textsuperscript{a,b}, and Dion Gijswijt\textsuperscript{a,c}

\textsuperscript{a}Centrum Wiskunde & Informatica, 1098 XG, Amsterdam, The Netherlands; \textsuperscript{b}Institute for Logic, Language and Computation, University of Amsterdam, 1098 XH, Amsterdam, The Netherlands; and \textsuperscript{c}Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, 2600 GA, Delft, The Netherlands

Edited by Robion C. Kirby, University of California, Berkeley, CA, and approved November 27, 2012 (received for review May 1, 2012)

The Shannon capacity of a graph $G$ is the maximum asymptotic rate at which messages can be sent with zero probability of error through a noisy channel with confusability graph $G$. This extensively studied graph parameter disregards the fact that on atomic scales, nature behaves in line with quantum mechanics. Entanglement, arguably the most counterintuitive feature of the theory, turns out to be a useful resource for communication across noisy channels. Recently [Leung D, Mancinska L, Matthews W, Ozols M, Roy A (2012) Commun Math Phys 311:97–111], two examples of graphs were presented whose Shannon capacity is strictly less than the capacity attainable if the sender and receiver have entangled quantum systems. Here, we give natural, possibly infinite, families of graphs for which the entanglement-assisted capacity exceeds the Shannon capacity.

Using the channel $\Theta(G)$ equals the maximum number of messages that can be transmitted when the sender and receiver share a pair of entangled quantum systems (the precise model is described below). Analogous to the classical setting, Cubitt et al. (5) defined the graph parameter $\alpha_q(G)$ (a quantum variant of the independence number) and proved that it equals the maximum number of pairwise nonconfusable messages that can be sent with a single use of a noisy channel and shared entanglement. They found examples of graphs for which $\alpha_q(G) > \alpha(G)$, showing that the use of entanglement can increase the “one-shot” zero-error capacity of a channel [more examples were found recently by Mančinska et al. (6)]. This result was surprising because entanglement cannot increase the standard capacity of a classical discrete memoryless channel (as shown by Bennett et al. (7)). Of course, the next question was if the entanglement-assisted capacity

$$\Theta_q(G) = \lim_{n \to \infty} \sqrt[n]{\alpha_q(G^\otimes n)}$$

could be strictly greater than the Shannon capacity. In contrast with the combinatorial nature of the Shannon capacity, the entanglement-assisted capacity can sometimes be

Author contributions: J.B. and H.B. designed research; J.B., H.B., and D.G. performed research; J.B., H.B., and D.G. contributed new reagents/analytic tools; and J.B., H.B., and D.G. wrote the paper.

The authors declare no conflict of interest.

1To whom correspondence should be addressed. E-mail: jop.briet@cwi.nl.
that if \( n \) is a large enough multiple of 4, then the independence number is less than \((2 - \varepsilon)^{n}\) for some \( \varepsilon > 0 \) independent of \( n \). However, despite effort from the quantum-information community, it remains unknown if this graph gives such a separation. Our main result shows that under certain conditions a separation holds for a "quarter" of the orthogonality graph.

**Our Results**

In this paper we present two natural, possibly infinite, families of basic graphs whose entanglement-assisted capacity exceeds the Shannon capacity. The graphs are defined as follows. Let \( H_n \) be the graph with as vertex set all binary strings of odd length \( n \) and even Hamming weight, and as edge set the pairs with Hamming distance \((n + 1)/2\). Let \( G_n \) be the subgraph of \( H_n \) induced by the strings of Hamming weight \((n + 1)/2\). We prove the following.

**Theorem 1.** Let \( p \) be an odd prime such that there exists a Hadamard matrix of size \( 4p \). Then, for \( n = 4p - 1 \) and \( G \) either \( G_n \) or \( H_n \), we have

\[
\Theta_q(G) / \Theta(G) \geq \Omega\left(\frac{p^{7/2}}{n^{3/2}}\right).
\]

Notice that the graph \( H_n \) is a subgraph of the orthogonality graph on \( \{0,1\}^{n+1} \), induced by the \((n+1)\)-bit strings with even Hamming weight and first coordinate equal to 0. Based on constructions of Hadamard matrices by Scarpir (14) and Paley (15), Theorem 1 holds for any prime \( p \) such that \( 4p - 1 = q^2 \) for some odd prime \( q \) and positive integer \( k \). The first three examples of such \( (p,q) \) pairs for \( k = 1 \) are \((3,11)\), \((5,19)\), and \((11,43)\). Examples for \( p \approx 10^{12} \) and \( k = 1 \) can readily be generated with little computing power. The subset of strings in the vertex set of \( G_n \) that have zeros on the last \((n - 7)/4 \) coordinates is an independent set of size \( \Omega(20^{2/5n}) \), showing that the Shannon capacity of \( G_n \) is exponential in \( n \). Because \( G_n \) is an induced subgraph of \( H_n \), the same holds for the latter graph.

We observe that the results of ref. 8 imply that the sequence of graphs \( (G^{2^k}_{2^k})_{k \geq 0} \) has a capacity ratio \( \Theta_q / \Theta \) that grows as roughly \( |V(G^{2^k}_{2^k})|^{0.101} \), where \( |V(G)| \) is the number of vertices of the graph \( G \) (the graph \( G_{2^k} \) gives better dependence on the number of vertices than \( G_{2^k} \), does). Our results show that the family of graphs \( G_n \) gives a slightly higher ratio of roughly \( |V(G_n)|^{0.187} \).

**Theorem 1** follows directly from the following lemmas, which give lower and upper bounds on the entanglement-assisted capacity and Shannon capacity, respectively.

**Lemma 1.** Let \( n \) be a positive integer such that there exists a Hadamard matrix of size \((n + 1)\). Then, for \( G \) either \( G_n \) or \( H_n \), we have

\[
\Theta_q(G) \geq \frac{|V(G)|}{(n + 1)^2}.
\]

**Lemma 2.** Let \( p \) be an odd prime and let \( n = 4p - 1 \). Then, for \( G \) either \( G_n \) or \( H_n \), we have

\[
\Theta(G) \leq \frac{n}{(n - 1)} + \frac{n}{(n - 2)} + \cdots + \frac{n}{(n - p - 1)}.
\]

Aside from relying on a few basic facts of graph theory and the theory of finite fields, our proofs of these lemmas are straightforward and self-contained. To obtain the asymptotic bound of **Theorem 1**, we upper-bound the binomial sum of Lemma 2 by the well-known estimate \( 2^{n(\log n)/\log 2} \), where \( H(t) = -t \log_2 t - (1 - t) \log_2 (1 - t) \) is the binary entropy function, and use the bound \( |V(G_n)| \geq \Omega(2^{n/\sqrt{n}}) \).

**Entanglement-Assisted Capacity of a Graph**

In this section we give the formal definition of the entanglement-assisted capacity of a graph. Let \( G \) be a finite simple undirected
graph, with vertex set $V(G)$ and edge set $E(G) \subseteq \binom{V}{2}$. The strong graph product $G \boxtimes H$ of two graphs $G$ and $H$ has as vertex set all pairs $(x, y) \in V(G) \times V(H)$. Two vertices $(x, y)$ and $(x', y')$ are adjacent in $G \boxtimes H$ if and only if $x$ and $x'$ are adjacent in $G$ or equal, and $y$ and $y'$ are adjacent in $H$ or equal. For example, if $(x, x') \in E(G)$ and $(y, y') \in E(H)$, then the four pairs $(x, y), (x, y'), (x', y), \text{ and } (x', y')$ form a 4-clique in $G \boxtimes H$. We denote by $G^{\otimes n}$ the $n$-fold strong graph product of $G$ with itself. Recall that the Shannon capacity of $G$ is defined as $\Theta(G) = \sup_n (\alpha(G^{\otimes n}))^1/n$.

The entanglement-assisted capacity of a graph is defined as follows.

**Definition 1. Entangled capacity of a graph:** Let $G = (V, E)$ be a graph. Define $\alpha_q(G)$ as the largest natural number $M$ such that there exists a Hilbert space $H$, a trace-1 positive semidefinite operator $\rho$ on $H$, and for every $i \in \{1, \ldots, M\}$ and $x \in V$, a positive semidefinite operator $\rho(x)_i$ on $H$ satisfying

1. $\sum_i \rho(x)_i = \rho$ for every $i \in \{1, \ldots, M\}$;
2. $\rho(x_i)\rho(x_j) = 0$ for every $x \in V$ and $i \neq j$;
3. $\rho(x_i)\rho(x_j) = 0$ if $\{x_i, x_j\} \in E$ and $i \neq j$.

The entanglement-assisted capacity of $G$ is defined by

$$\Theta_q(G) = \sup_n (\alpha_q(G^{\otimes n}))^1/n.$$ 

The parameter $\alpha_q(G)$ satisfies $\alpha_q(G) \geq \alpha(G)$ and is a generalization of the independence number. To see this, restrict in Definition 1 the space $H$ to be one-dimensional and add the restrictions $\rho = 1$ and $\rho(x), \rho(x_i) \in \{0, 1\}$. Say that a vertex $x \in V$ gets label $i$ if $\rho(x_i) = 1$. **Condition 1** says that exactly one vertex gets label $i$, **Condition 2** says that each vertex gets at most one label, and **Condition 3** says that no two adjacent vertices belong to the privileged subset of labeled vertices. Hence, the system $(\rho(x)_i)_{x,i}$ gives an independent set of size $M$, namely the set $\{x : \rho(x_i) = 1 \text{ for some } i\}$. Because $\alpha_q(G)$ relaxes this characterization of $\alpha(G)$, it follows that $\alpha_q(G) \geq \alpha(G)$.

By using tensor products of the operators $\rho$ and $\rho(x)$, it is not hard to see that $\alpha_q(G^{\otimes n})$ is nondecreasing with $k$. It follows that $\Theta_q(G) \geq \Theta(G)$ and (by Fekete’s Lemma) that $\Theta_q(G) = \lim_{n \to \infty} (\alpha_q(G^{\otimes n}))^1/n$.

**Entanglement-Assisted Communication**

In this section we describe the model of zero-error entanglement-assisted communication over classical channels. Readers who are familiar with this model or want to move on to the proof of the main result can safely skip this section. We start with some basic definitions of quantum-information theory. For more details we refer to Nielsen and Chuang (16).

**Shared Entangled States.** A state $\rho$ is a positive-semidefinite matrix whose trace equals 1. We identify a matrix of size $d \times d$ with a linear operator on $\mathbb{C}^d$ in the obvious way. A state should be thought of as describing the configuration of a quantum system: an abstract physical object, or a collection of objects, on which one can perform experiments. Associated with a quantum system $Q$ is a complex Euclidean vector space $Q = \mathbb{C}^n$, for some dimension $d$. The possible configurations of $Q$ are the states on $Q$.

Suppose the sender and receiver hold quantum systems $S$ and $R$, respectively. Associated with the sender’s system is a space $\mathcal{X} = \mathbb{C}^n$, and associated with the receiver’s system is a space $\mathcal{Y} = \mathbb{C}^m$. Then, by definition, the possible configurations of the joint system $(S, R)$ are the states on $\mathcal{X} \otimes \mathcal{Y}$. If the system $(S, R)$ is in the state $\rho$, then the sender and receiver are said to share the state $\rho$. A state on $\mathcal{X} \otimes \mathcal{Y}$ is entangled if it is not a convex combination of states of the form $\rho_S \otimes \rho_R$, where $\rho_S$ is a state on $\mathcal{X}$ and $\rho_R$ a state on $\mathcal{Y}$.

**Measurements.** Let $S$ be a finite set and let $Q$ be a quantum system with associated vector space $Q = \mathbb{C}^n$. A measurement on the system $Q$ with outcomes in $S$ is a system of positive semidefinite matrices $M^g$ on $Q$, $x \in S$, which satisfies

$$\sum_{x \in S} M^g = I_Q,$$

where $I_Q$ denotes the identity on $Q$.

Let $\{A^g \in \mathbb{C}^{n \times n} : x \in S\}$ be a measurement on the sender’s quantum system $S$. The numbers

$$p_x = \text{Tr}(A^g \otimes I_y)$$

define a probability distribution on $S$. This follows easily from the properties of the matrices $A^g$ and $\rho$ and the fact that for positive semidefinite matrices $A$ and $B$, we have $\text{Tr}(AB) \geq 0$.

**The partial trace function over $\mathcal{X}$ of a matrix $M$ on $\mathcal{X} \otimes \mathcal{Y}$ is defined by**

$$\text{Tr}_\mathcal{X}(M) = (I_\mathcal{Y} \otimes I_x)\text{Tr}(e_1 \otimes I_y)M(e_1 \otimes I_y) + \cdots + (e_m \otimes I_y)\text{Tr}(e_m \otimes I_y)M(e_m \otimes I_y),$$

where $e_1, \ldots, e_m$ are the canonical basis vectors for $\mathcal{X}$. This function yields an $n \times n$ matrix (i.e., a linear operator on the space $\mathcal{Y}$). It is not hard to see that the matrices

$$\rho(x) = \frac{\text{Tr}_\mathcal{X}(A^g \otimes I_y)\rho)}{p_x}$$

are each, in fact, states on the space $\mathcal{Y}$ associated with the receiver’s system $R$.

The postulates of quantum mechanics dictate that if the sender performs the measurement defined by the matrices $A^g$ on her system $S$, then the following two things happen:

1. She obtains outcome $x \in S$ with probability $p_x$.
2. The receiver’s system $R$ is left in the state $\rho(x)$ on $\mathcal{Y}$.

For some finite set $S$, the receiver can perform a measurement $\{B^a \in \mathbb{C}^{n \times n} : a \in \mathcal{R}\}$ on $R$, and he will obtain outcome “a” with probability $\text{Tr}(B^a \rho(x))$. The joint probability of the sender and receiver obtaining outcomes $x$ and $a$, respectively, is then given by $\text{Tr}(A^g \otimes B^a)$. If the state $\rho$ is not entangled, then this probability distribution is classical. Entanglement is thus necessary to obtain nonclassical quantum distributions.

**Entanglement-Assisted Communication.** To send messages across a noisy channel defined by input alphabet $S$, output alphabet $\mathcal{R}$, and conditional probability distribution $P$, the sender and receiver can use shared entanglement as follows. Let $\rho$ be a state shared between the sender and receiver. Let $M$ be a positive integer and for every $i \in \{1, \ldots, M\}$ let $\{A^g \in \mathbb{C}^{n \times n} : x \in S\}$ be a measurement on the sender’s system $S$ with outcomes in $S$. For every $a \in \mathcal{R}$, let $\{B^a \in \mathbb{C}^{n \times n} : a \in \mathcal{R}\}$ be a measurement on the receiver’s system $R$ with outcomes in $\{1, \ldots, M\}$. Suppose that for every $i \neq j$ and $(x, a) \in S \times \mathcal{R}$ such that $P(a|x) \neq 0$, we have

$$\text{Tr}(A^g \otimes B^a) = 0.$$ 

To communicate the index $i$, the sender can then perform the $i$th measurement on her system and send her outcome $x \in S$ through the channel. The receiver gets a message $a \in \mathcal{R}$ satisfying $P(a|x) \neq 0$. The above discussion shows that if the receiver then
performs the measurement labeled by a, he obtains outcome i with probability 1.

The link between this model and Definition 1 is given by the following theorem. Let us denote by $d'_b(S,R,P)$ the maximum number M such that a state $\rho$ and matrices $A'_b,B'_b$ with the above property exists.

**Theorem 2 (Cubitt et al. [5]).** Let $(S, R, P)$ be a noisy channel and let $G$ be its confusability graph. Then, $d'_b(S,R,P) = d_b(G)$.

**Preliminaries**

**Notation.** We use the following notation:

- For strings $x, y \in \{0,1\}^n$, let $d(x,y)$ denote their Hamming distance.
- For vectors $u, v \in \mathbb{R}^n$, let $u \cdot v$ denote their Euclidean inner product.
- For a prime number $p$, we write $\mathbb{F}_p$ for a finite field consisting of $p$ elements.
- For vectors $u, v \in \mathbb{F}_p^n$, let $(u,v)$ denote their inner product over $\mathbb{F}_p$.
- For a field $\mathbb{F}$, we denote by $[\mathbb{F}]:=[\mathbb{F}, \mathbb{F}, \ldots, \mathbb{F}]$ the ring of n-variate polynomials with coefficients in $\mathbb{F}$.

**Some Basic Graph Theory.** Let $G$ be a graph. A permutation of the vertices $\pi: V(G) \to V(G)$ is an automorphism of $G$ if for every $x, y \in V(G)$, the pair $\{\pi(x), \pi(y)\}$ is an edge if and only if $\{x, y\}$ is an edge. Let $\text{Aut}(G)$ denote the group of automorphisms of $G$. For $x \in V(G)$, the set $\text{Orb}(x) = \{\pi(x) : \pi \in \text{Aut}(G)\}$ is the orbit of $x$ and the set $\text{Stab}(x) = \{\pi \in \text{Aut}(G) : \pi(x) = x\}$ is the stabilizer of $x$.

**Definition 2:** A graph $G$ is vertex transitive if for every vertex $x \in V(G)$, we have $\text{Orb}(x) = V(G)$.

**Lemma 3. Orbit-Stabilizer Theorem (17).** Let $G$ be a graph and $x \in V(G)$. Then $|\text{Orb}(x)| \cdot |\text{Stab}(x)| = |\text{Aut}(G)|$.

**Corollary 3.** Let $G$ be a vertex transitive graph and $x, y \in V(G)$. Then, there are exactly $|\text{Aut}(G)|/|\text{Stab}(x)|$ automorphisms of $G$ that map $x$ to $y$.

**Proof:** Because $G$ is vertex transitive, there exists an automorphism $\pi \in \text{Aut}(G)$ such that $\pi(x) = y$. Consider the set of automorphisms $\pi \cdot \text{Stab}(x) = \{\sigma = \pi \cdot \sigma : \pi \in \text{Stab}(x)\}$. Clearly $\pi' = \pi \cdot \sigma$ for every $\pi' \in \pi \cdot \text{Stab}(x)$. We claim that $\pi \cdot \text{Stab}(x)$ contains all automorphisms that map $x$ to $y$. To see this, notice that for any $\pi' \in \text{Aut}(G)$ such that $\pi'(x) = y$, we have $\pi' \cdot \sigma \in \pi \cdot \text{Stab}(x)$ and hence $\pi' = \pi \cdot \sigma$. Because $\pi' = \sigma \pi'$ implies that $\sigma = \pi'$, we have $|\pi \cdot \text{Stab}(x)| = |\text{Stab}(x)|$. The claim follows because, by the Orbit-Stabilizer Theorem, we have $|\text{Orb}(x)| = |\text{Aut}(G)|/|\text{Orb}(x)|$, and by vertex transitivity of $G$, we have $|\text{Orb}(x)| = |V(G)|$.

**Lower Bounds on the Entanglement-Assisted Capacity**

In this section we lower-bound the entanglement-assisted capacity of the graphs $G_n$ and $H_n$. We start by dealing with the graph $G_n$. The graph $H_n$ will be treated afterward in a similar manner.

To prove the lower bounds, we use a straightforward general method which was also used before in refs. 5 and 8. Recall that a (real) $d$-dimensional orthonormal representation of a graph $G$ is a mapping $f : V(G) \to \mathbb{R}^d$ satisfying $f(x) \cdot f(x) = 1$ and $f(x) \cdot f(y) = 0$ for every $\{x,y\} \in E(G)$.

**Proposition 4.** If a graph $G$ has an orthonormal representation $f : V(G) \to \mathbb{R}^d$ and has $M$ disjoint $d$ cliques, then $\Theta_d(G) \geq M$.

**Proof:** Let $\{1, \ldots, M\}$ be a label set for the disjoint cliques. Let $\rho = I/d$, where $I$ is the $d \times d$ identity matrix. For every $x \in V$ and $i \in \{1, \ldots, M\}$ let $\rho(x) = f(x) f(x)^T / d$ if $x$ belongs to the $i$th clique and let $\rho(x)$ be the zero matrix otherwise. Clearly these matrices are positive semidefinite, and it is easy to check that they satisfy the conditions of Definition 1 using the fact that for every $d$-clique $C \subseteq V$, the set $\{f(x) : x \in C\}$ is a complete orthonormal basis for $\mathbb{R}^d$. This gives $\Theta_d(G) \geq \Theta_d(G) \geq M$.

The lower bounds on the entanglement-assisted capacity given in Lemma 1 follow immediately from the following two lemmas and Proposition 4.

**Lemma 4.** Let $n$ be an odd integer. Then, the graph $G_n$ has an $n$-dimensional orthonormal representation.

**Lemma 5.** Let $n$ be such that there exists a Hadamard matrix of size $n+1$. Then, the graph $G_n$ has at least $|V(G_n)|/n^2$ disjoint cliques of size $n$.

We proceed by proving these lemmas.

**Proof of Lemma 4:** Associate with every vertex $x = (x_1, \ldots, x_n) \in V$ a sign vector given by $u[x] = ((-1)^{x_1}, \ldots, (-1)^{x_n}) \in \mathbb{R}^n$. Let $1$ denote the $n$-dimensional all-ones vector. Note that for every $x \in V$, we have $u[x] \cdot 1 = -1$, as the Hamming weight of $x$ is $(n+1)/2$. Moreover, for every $\{x,y\} \in E$ we have $u[x] \cdot u[y] = -1$, which follows from the fact that $d(x,y) = (n+1)/2$.

Now consider the $(n+1)$-dimensional unit vectors $f(x) = (u[x] \otimes 1)/\sqrt{n+1}$ (i.e., the column vector $u[x]$ with a 1 appended to it, normalized). These vectors satisfy
1. For every $\{x,y\} \in E$ we have $f(x) \cdot f(y) = (u[x] \otimes 1) \cdot (u[y] \otimes 1) = 0$.
2. For every $x \in V$ we have $f(x) \cdot (1 \otimes 1) = (u[x] \otimes 1) \cdot (1 \otimes 1) = -1 + 1 = 0$.

The first item shows that $f$ forms an orthonormal representation of $G$. The second item says that the vectors $(f(x))_{x \in V}$ lie on a single $n$-dimensional hyperplane (orthogonal to the all-ones vector). Hence these vectors span a space of dimension at most $n$. It follows that there is an $n$-dimensional orthonormal representation of $G_n$.

To prove Lemma 5, we need to find a large number of disjoint $n$ cliques in $G_n$. We achieve this by first finding just one $n$ clique. Using the fact that $G_n$ is vertex transitive, we show that the existence of a single clique implies the existence of many disjoint cliques. More explicitly, one can produce many pairwise disjoint $n$ cliques by simultaneously permuting the coordinates of the strings in this one clique. Notice that this permutation operation leaves both the Hamming weights and the Hamming distances invariant. A suitable choice of such permutations gives pairwise disjoint cliques from any single clique, as whether or not a set of $n$-bit strings forms a clique in $G_n$ depends only on their Hamming weights and Hamming distances.

The following proposition tells us when we can find a single $n$ clique in $G_n$.

**Proposition 5.** Let $n$ be such that there exists a Hadamard matrix of size $(n+1)$. Then, there exists an $n$ clique in $G_n$.

**Proof:** Let $M$ be an $(n+1) \times (n+1)$ Hadamard matrix. We may assume that the first row and column of $M$ contain only $+1$’s, because multiplying all entries in a row (or column) by $-1$ gives again a Hadamard matrix. Because each of the last $n$ rows of $M$ is orthogonal to the first row, it has exactly $(n+1)/2$ entries equal to $-1$. Moreover, because each pair from the last $n$ rows of $M$ is orthogonal, the two rows differ in exactly $(n+1)/2$ coordinates.
Let $C$ be the $n \times n$ matrix obtained by removing the first row and column from $M$. Then, each row of $C$ has exactly $(n + 1)/2$ entries equal to $-1$, and every pair of rows from $C$ differs in exactly $(n + 1)/2$ coordinates. Hence, the rows of $C$ are a clique in $G_n$.

Next, we lower-bound the number of disjoint $n$ cliques of size $n$ in $G_n$. We use the following lemma and proposition.

**Lemma 6.** Let $G$ be a vertex transitive graph that has a $d$ clique as an induced subgraph. Then, $G$ has at least $|V(G)|/d^2$ vertex-disjoint $d$ cliques.

**Proof.** Let $W = C_1 \cup C_2 \cup \ldots \cup C_k$ be a union of $k$ disjoint $d$ cliques, with $k$ maximal. Because $G$ is vertex transitive, Corollary 3 implies that for every pair of vertices $u, v$ there are exactly $|\text{Aut}(G)|/|V(G)|$ automorphisms mapping $u$ to $v$. It follows that at most

$$|W| \cdot |C_1| \cdot |\text{Aut}(G)|/|V(G)|$$

automorphisms map a vertex in $C_1$ to a vertex in $W$.

On the other hand, by maximality of $k$, $\sigma(C_1) \cap W$ is nonempty for every automorphism $\sigma$. It follows that $|W| \cdot |C_1| \geq |V|$, and hence $k \leq |W|/|C_1| \geq |V|/|C_1| = |V|/d^2$.

**Proposition 6.** For every $n$, the graph $G_n$ is vertex transitive.

**Proof.** Consider the group $S_n$ of permutations on $\{1, \ldots, n\}$. For every $\sigma \in S_n$, define the map $\Gamma_n : \{0, 1\}^n \rightarrow \{0, 1\}^n$ by $\Gamma_n(x) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. As $\Gamma_n$ leaves the Hamming weight invariant, we have $\Gamma_n : V(G_n) \rightarrow V(G_n)$. Moreover, $\Delta(\Gamma_n(x), \Gamma_n(y)) = \Delta(x, y)$. Hence, $\Gamma_n \in \text{Aut}(G_n)$. Finally, for every $x \in V(G_n)$ we have $\{\Gamma_n(x) : x \in S_n\} = V(G_n)$, and we are done.

**Proof of Lemma 5:** The result follows by combining Propositions 5 and 6 and Lemma 6.

We deal with the graphs $H_n$ in the same way as we did with the graphs $G_n$. We directly obtain the result of Lemma 1 for these graphs by combining the following two lemmas with Proposition 4.

**Lemma 7.** Let $n$ be an odd integer. Then, $H_n$ has an orthonormal representation of dimension $n + 1$.

**Lemma 8.** Let $n$ be such that there exists a Hadamard graph of size $n$. Then, the graph $H_n$ has at least $|V(H_n)|/(n + 1)^2$ disjoint cliques of size $n + 1$.

**Proof of Lemma 7:** Associate with every vertex $x = (x_1, \ldots, x_n) \in V$ the vector

$$u[x] = (-1)^{x_1}, \ldots, (-1)^{x_n}^T$$

Then, the unit vectors $f(x) = (u[x] \otimes 1)/\sqrt{n + 1}$ form an $(n + 1)$-dimensional orthonormal representation of $H_n$.

To prove Lemma 8 we proceed as in the proof of Lemma 5: We first find a single $(n + 1)$-clique in $H_n$. Then, we prove that $H_n$ is vertex transitive and use Lemma 6.

**Proposition 7.** Let $n$ be such that there exists a Hadamard matrix of size $(n + 1)$. Then, there exists an $(n + 1)$ clique in $H_n$.

**Proof:** Let $n$ be an odd integer. Then, because each of the vertices in $C$ has Hamming weight $(n + 1)/2$, the union of $C$ and the all-zeros string gives an $(n + 1)$ clique in $H_n$. The result now follows from Proposition 5.

**Proposition 8.** For every $n$, the graph $H_n$ is vertex transitive.

**Proof:** Recall that $V(H_n) \subseteq \mathbb{F}_2^n$ consists of the strings of even Hamming weight. For every $x \in V(H_n)$ define the linear bijection $\Sigma : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ by $\Sigma(x) = x + z$. As $\Sigma$ leaves the parity of Hamming weight invariant, we have $\Sigma : (H_n) \rightarrow (H_n)$. Moreover, $\Delta(\Sigma(x), \Sigma(y)) = \Delta(x, y)$. Hence, $\Sigma \in \text{Aut}(G_n)$. For every $x \in V(H_n)$ we have $\{\Sigma(x) : \sigma \in \text{Aut}(G_n)\} = V(H_n)$, and we are done.

**Proof of Lemma 8:** The result follows by combining Propositions 7 and 8 and Lemma 6.

**Upper Bounds on the Shannon Capacity**

In this section we upper-bound the Shannon capacity of the graphs $G_n$ and $H_n$. We recall that $G_n$ has as vertex set all binary strings of odd length $n$ and Hamming weight $(n + 1)/2$, and as edges the set of vertices with Hamming distance $(n + 1)/2$. The graph $H_n$ has as vertex set all binary strings of odd length $n$ and even Hamming weight, and as edges the set of vertices with Hamming distance $(n + 1)/2$. The proof of the upper bounds in Lemmas 2 is based on a general method of Haemers (18) and an algebraic lemma of Frankl and Wilson (19).

**Lemma 9 (Haemers).** Let $G = (V, E)$ be a graph. Let $F$ be a field. Let $A : V \times V \rightarrow F$ be a matrix such that for every $x \in V$ we have $A(x, x) \neq 0$ and for every nonadjacent pair $x, y \in V$ we have $A(x, y) = 0$. Then, $\Theta(G) \leq \text{rank}(A)$.

**Proof:** Say that a matrix $A : V \times V \rightarrow F$ fits $G$ if it satisfies the conditions stated in the lemma. Let $S \subseteq V$ be a maximum-sized independent set and let $A$ be a matrix that fits $G$. Then, the principal submatrix of $A$ defined by $S$ has rank $|S|$. Hence, we have $\text{rank}(A) \leq \text{rank}(S)$. The result follows because $A^{2n}$ fits $G^{2n}$ and $\text{rank}(A^{2n}) = \text{rank}(A^n)$.

We say that a polynomial is multilinear if its degree in each variable is at most 1.

**Lemma 10 (Frankl–Wilson).** Let $p$ be an odd prime, let $r$ be a natural number, and let $n = rp - 1$. Let $V \subseteq \{-1, 1\}^p \subseteq \mathbb{F}_p$ be a set of vectors over $\mathbb{F}_p$. Then, for every $u \in V$ there exists a multilinear polynomial $P_u \in \mathbb{F}_p[v_1, \ldots, v_n]$ satisfying

1. $P_u(u) \neq 0$.
2. For every $v \in V$ such that $\langle u, v \rangle \neq -1$, we have $P_u(v) = 0$.
3. $\deg(P_u) \leq p - 1$.

**Proof:** For every vector $u \in V$ let $Q_u \in \mathbb{F}_p[v_1, \ldots, v_n]$ be the polynomial defined by

$$Q_u(v) = \prod_{i=1}^{p-1} (\langle u, v \rangle + 1 - 1).$$

Because $n \equiv -1 (mod p)$, every $v \in V$ satisfies $\langle v, v \rangle = -1$. By Wilson’s Theorem [for example, Lidl and Niederreiter (20)], it follows that $Q_u(u) = (-1)^{p-1}(p-1) = -1$. If $\langle u, v \rangle \neq -1$ we have $Q_u(v) = 0$ because in this case we have $\langle u, v \rangle + 1 \in \{1, \ldots, p - 1\}$. In particular, we have $Q_u(u) \neq 0$. Because $\langle u, v \rangle$ is a linear function, we have $\deg(Q_u) = p - 1$.

Define the multilinear polynomial $P_u$ by expanding $Q_u$ in the monomial basis and changing the powers of $t_i$ in the monomial $t_1^{1}\cdots t_n^{1}$ to 0 if $t_i$ is even and to 1 if $t_i$ is odd. Then, $P_u$ is multilinear and agrees with $Q_u$ everywhere on $\{-1, 1\}^n$ and satisfies $\deg(P_u) \leq \deg(Q_u)$.

We now show how these two lemmas can be combined to give Lemma 2, which states that for $p$ an odd prime and $n = 4p - 1$, and $G$ either $G_n$ or $H_n$, we have $\Theta(G) \leq O((24/25)^{n/2})$.

**Proof of Lemma 2:** Let $F$ be either $G_n$ or $H_n$. For every $x \in V$ let $u(x) = (\langle x, 1 \rangle^{1}, \ldots, \langle x, n \rangle^{1})$ be the corresponding sign vector in $\mathbb{F}_2^n$. Because $n = 4p - 1 \equiv -1 (mod p)$ and $\mathbb{F}_p$ is isomorphic to the ring of integers mod $p$, we have for every $x, y \in V$

$$\langle u[x], u[y] \rangle = -2d(x, y) = -2d(x, y) - 1.$$
Hamming distance \(2p\), we have \(2d(x, y) \neq 4p\). This implies that \(2d(x, y) \neq 0 \pmod{p}\), and the claim follows from Eq. 1.

Set \(r = 4\) and let \(V = \{ x[1] : x \in V \} \). Then, \textbf{Lemma 10} gives a multilinear polynomial \(P_e \in \F_p[v_1, \ldots, v_n] \) for every \(x \in V\), satisfying

1. \(P_e(u[x]) = 0\);
2. For every \(y \in V\) such that \(y \neq x\) and \(\{x, y\} \notin E\), we have \(P_e(u[y]) = 0\);
3. \(\deg(P_e) \leq p - 1\).

The set \(M\) of multilinear monomials in \(n\) variables of degree at most \(p - 1\) forms a basis for the space of multilinear polynomials of degree at most \(p - 1\). For every vertex \(x \in V\), define vectors \(S[x], T[x] \in \F^M_p\) as follows. For monomial \(m \in M\) let \(S[x][m]\) be the coefficient of \(m\) in the expansion of the polynomial \(P_e\) in the basis \(M\), and let \(T[x][m] = m(u[x])\) be the value obtained by evaluation the monomial \(m\) at \(u[x]\). Then, for every \(x, y \in V\) we have \(S[x] \cdot T[y] = P_e(u[y])\).

Consider now the matrix \(A : V \times V \rightarrow \F_p\) defined by \(A(x, y) = S[x] \cdot T[y]\). Because the vectors \(S[x]\) and \(T[y]\) have dimension \(|M|\), we have \(\text{rank}(A) \leq |M|\). Additionally, it follows from the properties of the polynomials \(P_e\) that the matrix \(A\) satisfies \(A(x, x) \neq 0\) for every \(x \in V\) and \(A(x, y) = 0\) for every nonadjacent pair \(x, y \in V\).

The claim now follows from \textbf{Lemma 9} and the fact that

\[
|M| = \sum_{i=0}^{p-1} \binom{n}{i}.
\]

This completes the proof.

**ACKNOWLEDGMENTS.** J.B. thanks Oded Regev for discussions at Ecole Normale Supérieure Paris and for comments on the manuscript. We thank Monique Laurent and David Garcia Soriano for discussions and Lex Schrijver for literature pointers. Work supported by the European Union Seventh Framework Programme Grant QCS (to J.B. and H.B.).