Unextendible Product Bases

N. Alon *   L. Lovász †

February 22, 2002

Abstract

Let C denote the complex field. A vector v in the tensor product $\otimes_{i=1}^{m} C^{k_i}$ is called a *pure product vector* if it is a vector of the form $v_1 \otimes v_2 \cdots \otimes v_m$, with $v_i \in C^{k_i}$. A set F of pure product vectors is called an *unextendible product basis* if F consists of orthogonal nonzero vectors, and there is no nonzero pure product vector in $\otimes_{i=1}^{m} C^{k_i}$ which is orthogonal to all members of F. The construction of such sets of small cardinality is motivated by a problem in quantum information theory. Here it is shown that the minimum possible cardinality of such a set F is precisely $1 + \sum_{i=1}^{m}(k_i - 1)$ for every sequence of integers $k_1, k_2, \ldots, k_m \geq 2$ unless either (i) $m = 2$ and $2 \in \{k_1, k_2\}$ or (ii)$1 + \sum_{i=1}^{m}(k_i - 1)$ is odd and at least one k_i is even. In each of these two cases, the minimum cardinality of the corresponding F is strictly bigger than $1 + \sum_{i=1}^{m}(k_i - 1)$.

1 Introduction

Let C denote the complex field. A vector v in the tensor product $\otimes_{i=1}^{m} C^{k_i}$ is called a *pure product vector* if it is a vector of the form $v_1 \otimes v_2 \cdots \otimes v_m$, with $v_i \in C^{k_i}$. A set F of pure product vectors is called an *unextendible product basis (UPB)* if F consists of orthogonal nonzero vectors, and there is no nonzero pure product vector in $\otimes_{i=1}^{m} C^{k_i}$ which is orthogonal to all members of F. Note that the inner product of two pure product vectors is easy to express:

$$(u_1 \otimes \cdots \otimes u_m) \cdot (v_1 \otimes \cdots \otimes v_m) = (u_1 \cdot v_1) \cdots (u_m \cdot v_m).$$

Clearly there are trivial sets as above consisting of $\prod_{i=1}^{m} k_i$ vectors. Motivated by a question in quantum information theory concerning properties of entangled quantum states, the authors of [1], [5] were interested in smaller families. Let $f_m(k_1, k_2, \ldots, k_m)$ denote the minimum possible cardinality of such a family. It is easy to see that $f_m(k_1, \ldots, k_m) \geq 1 + \sum_{i=1}^{m}(k_i - 1)$. Indeed, if

$$\mathbf{v_j} = v_j^{(1)} \otimes v_j^{(2)} \otimes \cdots \otimes v_j^{(m)}, \quad 1 \leq j \leq \sum_{i=1}^{m}(k_i - 1)$$

*Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Email: noga@math.tau.ac.il. Research supported in part by a USA Israeli BSF grant, by a grant from the Israel Science Foundation and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University.

†Microsoft Research. One Microsoft Way, Redmond, WA 98052, USA. Email: lovasz@microsoft.com.

are pairwise orthogonal vectors, split the set of indices $I = \{1, 2, \ldots, \sum_{i=1}^{m}(k_i - 1)\}$ into m pairwise disjoint sets $I_1, I_2, \ldots, I_m$, where $|I_s| = k_s - 1$ for all s. Let $u_s \in C^{k_s}$ be a nonzero vector orthogonal to $v_j^{(s)}$ for all $j \in I_s$, and note that the vector $u_1 \otimes u_2 \otimes \ldots \otimes u_m$ is a pure product nonzero vector which is orthogonal to all vectors $\mathbf{v_j}$, implying that, indeed, $f_m(k_1, \ldots, k_m) > \sum_{i=1}^{m}(k_i - 1)$, as claimed.

The authors of ([1], [5]) constructed several examples showing that sometimes this inequality is tight. More precisely, they showed that $f_2(k, k) = 2k - 1$ for $k = 3, 7$ and 9, and conjectured that this holds for all $k = (p+1)/2$, with p being a prime congruent to 1 modulo 4. They also proved that $f_3(3, 3, 3) = 7$.

Here we observe that constructions of small maximal orthogonal families can be obtained by appropriate orthogonal representations of graphs, a notion introduced by the second author [6] in his study of the Shannon capacity of graphs. Applying this observation to appropriate representations of the Paley graphs we prove the above mentioned conjecture (using an explicit construction, suggested in [5]). More generally, combining the observation with the main result of [7] and certain known results in additive number theory we obtain a much stronger result. Note that in the study of $f_m(k_1, \ldots, k_m)$ we may always assume that $k_i \geq 2$ for all i. Our main result is the following.

Theorem 1.1 *For every $m \geq 2$ and every sequence of integers $k_1, k_2, \ldots, k_m \geq 2$, $f_m(k_1, \ldots, k_m) = 1 + \sum_{i=1}^{m}(k_i - 1)$ unless either*
(i) $m = 2$ and $2 \in \{k_1, k_2\}$ or
(ii)$1 + \sum_{i=1}^{m}(k_i - 1)$ is odd and at least one k_i is even.
In each of these two cases, $f_m(k_1, \ldots, k_m)$ is strictly bigger than $1 + \sum_{i=1}^{m}(k_i - 1)$.

The rest of this paper is organized as follows. In Section 2 we prove, without any reference to orthogonal representations, that $f_2(k, k) = 2k - 1$ for all $k = (p+1)/2$ where p is a prime congruent to 1 modulo 4. This is done by an explicit, simple construction (which appears in [5]), and the desired properties are derived from some simple properties of Gauss sums and a known result of Čebotarev, thus proving conjecture 3 in [5]. Section 3 contains the connection between unextendible product bases and orthogonal representations of graphs, and provides a graph theoretic characterization of all m-tuples $(k_1, \ldots, k_m)$ for which $f_m(k_1, \ldots, k_m) = 1 + \sum_{i=1}^{m}(k_i - 1)$. In Section 4 we combine this characterization with certain constructions and known results in additive number theory to prove Theorem 1.1. The final Section 5 contains some concluding remarks.

2 A construction for $k = (p+1)/2$, $p \equiv 1 \pmod 4$ prime

Let p be a prime, $p \equiv 1$ (mod 4), and let $w = e^{\frac{2\pi i}{p}}$ be a primitive p-th root of unity. It is well known (see, e.g., [4], Chapter 2) that

$$\sum_{j \in Z_p} w^{j^2} = \sqrt{p}. \tag{1}$$

Let P denote the set of all nonzero quadratic residues in the finite field Z_p, and put $P = \{\alpha_2, \alpha_3, \ldots, \alpha_k\}$, where $k = (p+1)/2$. Let $N = Z_p - (\{0\} \cup P)$ be the set of all quadratic nonresidues. By (1)

$$\sum_{\alpha \in P} w^{\alpha} = \frac{\sqrt{p} - 1}{2},$$

and hence

$$\sum_{\beta \in N} w^{\beta} = \frac{-\sqrt{p}-1}{2}.$$

Define $a = (\frac{\sqrt{p}+1}{2})^{1/2}$. For each $j \in Z_p$ define a vector $u_j \in C^k$ by $u_j = (a, w^{j\alpha_2}, w^{j\alpha_3}, \ldots, w^{j\alpha_k})$. Notice that the product of u_j and u_s is

$$(u_j, u_s) = a^2 + \sum_{\alpha \in P} w^{(j-s)\alpha},$$

which is zero if (and only if) $j - s \in N$ (since in this case the set $\{(j-s)\alpha : \alpha \in P\}$ is simply N.) Fix some $\beta \in N$ and define, for each $j \in Z_p$, $v_j = u_{j\beta}$. Then $(v_j, v_s) = (u_{j\beta}, u_{s\beta})$ is zero if (and only if) $(j-s)\beta \in N$, namely, iff $j - s \in P$. It follows that the p vectors $u_j \otimes v_j$, $(j \in Z_p)$, are pairwise orthogonal. We claim that they form an UPB, that is, there is no nonzero pure product vector in $C^k \otimes C^k$ orthogonal to all of them. Indeed, suppose $u \otimes v \in C^k \otimes C^k$ is orthogonal to all of them. Then either u is orthogonal to at least k of the vectors u_j, or v is orthogonal to at least k of the vectors v_j (which form a permutation of the vectors u_j). We need the following fact:
Claim: Every set of k of the vectors u_j is linearly independent.
Proof: By a result of Čebotarev (c.f., e.g., [10] for a proof and several references and [11], page 505 for another proof) every square submatrix of the p by p matrix $W = (w^{ij} : i, j \in Z_p)$ is nonsingular. Since every matrix whose rows are k of the vectors u_j is obtained from a k by k square submatrix of W by multiplying the first column by a, the desired claim follows.
By the last claim it thus follows that only the zero vector can be orthogonal to k of the vectors u_j, implying that either $u = 0$ or $v = 0$, and completing the proof that the constructed set is an UPB, as needed. $\square$

3 Orthogonal representations of graphs

An *orthogonal representation* of an undirected graph $G = (V, E)$ is an assignment of a nonzero (real) vector to any vertex of the graph so that vectors assigned to non-adjacent vertices are orthogonal. This notion was introduced by the second author [6], who considered such representations (over the real field) in the study of the Shannon capacity of graphs. We next note that such representations are relevant to our question here. Let $K_n = (V, E)$ denote the complete graph on the set of vertices $V = \{1, 2, \ldots, n\}$. Given an edge coloring $c : E \mapsto \{1, \ldots m\}$ of K_n by m colors, let G_i denote the graph on V in which for $1 \leq s < t \leq n$ the vertices s and t are **not** adjacent iff the color of the edge st is i. The coloring c is called $(d_1, d_2, \ldots, d_m)$-*connected* if for every i the graph G_i is d_i-connected. The main result of this section is the following.

Theorem 3.1 *Let $m, k_1, \ldots, k_m$ be positive integers. Then $f_m(k_1, \ldots, k_m) = 1 + \sum_{i=1}^{m}(k_i - 1)$ if and only if for $n = 1 + \sum_{i=1}^{m}(k_i - 1)$ there is an $(n-k_1, n-k_2, \ldots, n-k_m)$-connected edge coloring of K_n.*

The main tool in the proof of the above theorem is the following result of Lovász, Saks and Schrijver (a correction of an error in the proof of this result was recently given in [8]).

Theorem 3.2 ([7, 8]) *Let G be a graph on n vertices. Then G is k-connected if and only if there is an orthogonal representation (over the reals) of G, assigning to each vertex a vector in R^{n-k} so that every set of $n-k$ vectors is linearly independent.*

Proof of Theorem 3.1: Suppose there is an $(n-k_1, n-k_2, \ldots, n-k_m)$-connected coloring $c : E \mapsto \{1, 2, \ldots, m\}$ of $K_n = (V, E)$, where $n = 1 + \sum_{i=1}^{m}(k_i - 1)$. Let G_i be the graph on V in which each pair of distinct vertices s, t are non-adjacent iff the color of st is i. By assumption G_i is $(n - k_i)$-connected. Therefore, by Theorem 3.2, there are vectors $v_1^{(i)}, v_2^{(i)}, \ldots, v_n^{(i)} \in R^{k_i}$ ($\subset C^{k_i}$) such that every set of k_i of them is linearly independent, and if the color of st is i, then the vectors $v_s^{(i)}$ and $v_t^{(i)}$ are orthogonal. It follows that the pure product vectors

$$\mathbf{v_j} = v_j^{(1)} \otimes v_j^{(2)} \otimes \cdots \otimes v_j^{(m)}, \quad 1 \leq j \leq n, \tag{2}$$

are pairwise orthogonal. Moreover, if $u_1 \otimes u_2 \otimes \cdots \otimes u_m$ is orthogonal to all of them then, by the pigeonhole principle, there is an index i such that u_i is orthogonal to at least k_i of the vectors $v_j^{(i)}$, and as these vectors are linearly independent it follows that u_i is the zero vector. This shows that the above collection is indeed an UPB, proving that $f_m(k_1, \ldots, k_m) \leq 1 + \sum_{i=1}^{m}(k_i - 1)$. Since the converse inequality always holds, it follows that in this case

$$f_m(k_1, \ldots, k_m) = 1 + \sum_{i=1}^{m}(k_i - 1), \tag{3}$$

as needed.

Conversely, suppose that (3) holds, put $n = 1 + \sum_{i=1}^{m}(k_i - 1)$ and let the vectors in (2) be an UPB in $C^{k_1} \otimes \cdots \otimes C^{k_m}$. Define an edge coloring c of K_n by m colors, by letting the color of the edge st be the first index i such that $v_s^{(i)}$ and $v_t^{(i)}$ are orthogonal. To complete the proof, we show that the graph G_i consisting of all edges whose color is not i is $(n - k_i)$-connected.

Suppose it is not, then one can separate two nonempty subsets S and T of vertices of G_i by removing $n - k_i - 1$ vertices. Therefore $|S| + |T| = k_i + 1$ and the two sets of vectors $V_S = \{v_s^{(i)}, s \in S\}$ and $V_T = \{v_t^{(i)}, s \in T\}$ are orthogonal (since all edges connecting S and T are colored i.) It follows that $\dim(V_S) + \dim(V_T) \leq k_i < |V_S| + |V_T|$ and hence we may assume, without loss of generality, that $\dim(V_S) < |V_S|$. By adding an arbitrary set of $k_i - |S|$ additional indices to the set S we obtain a set J_i of k_i indices such that the vectors $v_j^{(i)}, j \in J_i$ do not span C^{k_i}. We can now split arbitrarily all the remaining indices to sets of cardinalities $k_h - 1$ to obtain a partition $V = J_1 \cup J_2 \cup \ldots \cup J_m$, with $|J_i| = k_i$ and $|J_s| = k_s - 1$ for all $s \neq i$, such that for all $1 \leq s \leq m$, the set of vectors $v_j^{(s)}, j \in J_s$ does not span C^{k_s}. Therefore, there is a pure product nonzero vector

$$u_1 \otimes u_2 \otimes \cdots \otimes u_m \in \otimes_{s=1}^{m} C^{k_s},$$

where each u_s is orthogonal to all vectors $v_j^{(s)}$, $j \in J_s$, showing that the vectors $\mathbf{v_j}$ do not form an UPB, and contradicting the hypothesis. Therefore, G_i is $(n - k_i)$-connected, completing the proof. □

4 Connected edge colorings

The following is an easy consequence of Theorem 3.1.

Corollary 4.1 *Let $m, k_1, \ldots, k_m \geq 2$ be integers, and put $n = 1 + \sum_{i=1}^{m}(k_i - 1)$.*
(i) If at least one of the integers k_i is even and $n = 1 + \sum_{i=1}^{m}(k_i - 1)$ is odd, then $f_m(k_1, \ldots, k_m) > n$.
(ii) If $m = 2$ and $2 \in \{k_1, k_2\}$ then $f_2(k_1, k_2) > n$ $(= k_1 + k_2 - 1)$.

Proof: Suppose $f_m(k_1, \ldots, k_m) = n$. By Theorem 3.1 there is an $(n - k_1, \ldots, n - k_m)$-connected edge coloring of $K_n = (V, E)$. Let G_i denote the graph on V whose edges are all edges of K_n whose color is not i. As G_i is $(n - k_i)$-connected, it follows that its minimum degree is at least $n - k_i$. Therefore, there are at most $k_i - 1$ edges of color i incident with each vertex of K_n. Since $n - 1 = \sum_{i=1}^{m}(k_i - 1)$ this implies that there are precisely $k_i - 1$ edges of color i incident with each vertex. Consider, now, the two cases (i) and (ii) separately.
(i) Without loss of generality assume k_1 is even. Then, the complement of G_1 is a regular graph with an odd degree of regularity and an odd number of vertices, and this is impossible. Thus $f_m(k_1, \ldots, k_m) > n$, as needed.
(ii) Without loss of generality assume $k_1 = 2$. Then the complement of G_1 is a connected 1-regular graph on $n \geq 3$ vertices, and this is impossible showing that indeed $f_2(k_1, k_2) > n$. □

In order to apply Theorem 3.1 to prove that $f_m(k_1, \ldots, k_m) = 1 + \sum_{i=1}^{m}(k_i - 1)$ in all other cases we need a method for constructing connected edge colorings of K_n. The most convenient way to generate such colorings is by using Cayley graphs. Recall that the Cayley graph of an abelian finite group C with respect to the set $S \subset C$ that satisfies $S = -S$, $0 \notin S$ is the graph whose vertices are all members of C where $a, b \in C$ are connected iff $a - b \in S$. This is an $|S|$-regular graph. In certain cases it can be shown that it is $|S|$-connected. This can be done either by combinatorial techniques or by using tools from additive number theory; here we use both approaches.

Lemma 4.2 *Let n be a positive integer, suppose $2t \leq n - 3$ and let*

$$S = Z_n - \{-t, -(t-1), \ldots, 0, 1, \ldots (t-1), t\}.$$

Then, the Cayley graph of Z_n with respect to the set S is $|S|$-connected.

Proof: Suppose this is false. Then the complement of the graph contains a complete bipartite graph H with $2t + 2$ vertices. Call the two color-classes "red" and "blue".

Consider a red vertex u and a blue vertex v closest in the cyclic order. Suppose there are p uncolored vertices between them. Let u' be the vertex at distance t from u, measured away from v; let v' be defined analogously.

Since every colored vertex must be connected to either u or v, they are on the two arcs $[u, u']$ and $[v, v']$ which are of length $t + 1$ each. The total number of vertices on these arcs is at most $2t + 2$ and hence

$$\text{all vertices on these two arcs are colored.} \tag{4}$$

These two arcs cannot overlap or touch at u' and v'. Indeed, if they do, then all vertices of H are on an arc, implying that $p = 0$, and hence that $n \leq 2t + 2$, which contradicts the assumption $2t \leq n - 3$.

If the arc $[u, u']$ is all-red, and the arc $[v, v']$ is all-blue, then it is trivial to see that we have a red vertex and a blue vertex farther than t apart, which is impossible.

If one of these arcs is not monochromatic, then, by the minimality in the choice of u, v, $p = 0$. Let u'' and v'' be a pair of consecutive red and blue vertices on this arc. Replacing u and v by u'' and v'', we get a contradiction with (4) above. $\square$

The following theorem characterizes all pairs of integers k, r for which $f_2(k, r) = k + r - 1$.

Theorem 4.3 *For every two integers $k, r \geq 2$,*

$$f_2(k, r) = k + r - 1$$

if and only if $k > 2,\ r > 2$ and at least one of the two numbers is odd.

Proof: Put $n = k + r - 1$. By Corollary 4.1, if $f_2(k, r) = k + r - 1$ then both k and r exceed 2 and at least one of them is odd. To prove the converse, suppose $k, r > 2$ and assume, without loss of generality, that k is odd. Define $k - 1 = 2t$, $T = \{-t, -(t-1), \ldots, -1, 1, \ldots (t-1), t\}$ and $S = Z_n - (\{0\} \cup T)$. Then the Cayley graph of Z_n with respect to S is $|S| = (n - k)$-connected, by Lemma 4.2, whereas the Cayley graph of Z_n with respect to T is $|T| = (n - r)$-connected, by a simple, well known result (c.f., e.g., [2], pp. 47-49.) It thus follows, by Theorem 3.1, that indeed $f_2(k, r) = k + r - 1$. $\square$

The following well known theorem of Kneser (c.f., e.g., [9]) has numerous applications in additive number theory.

Theorem 4.4 (Kneser) *Let A, B be subsets of an abelian group G. Let $H = \{x : x + A + B = A + B\}$. Then $|A + B| \geq |A + H| + |B + H| - |H|$.*

Lemma 4.5 *For any sequence of odd integers $k_1, \ldots, k_m \geq 2$,*

$$f_m(k_1, k_2, \ldots, k_m) = 1 + \sum_{i=1}^{m} (k_i - 1).$$

Proof: By renumbering, if needed, the integers k_i, we may assume that $k_m \geq k_1 \geq k_2 \geq \ldots \geq k_{m-1}$. Put $n = 1 + \sum_{i=1}^{m} (k_i - 1)$ and $k_i - 1 = 2t_i$ for all $1 \leq i \leq m$. Note that n is odd. Split the integers $1, 2, \ldots, (n-1)/2$ into disjoint intervals of consecutive elements of sizes $t_1, t_2, \ldots, t_m$, that is, define $z_0 = 0,\ z_i = \sum_{j=1}^{i} t_j$ and $I_i = \{z_{i-1} + 1, z_{i-1} + 2, \ldots, z_{i-1} + t_i = z_i\}$. Put, also, $T_i = I_i \cup (-I_i)$, and $S_i = Z_n - (\{0\} \cup T_i)$. To complete the proof it suffices, in view of Theorem 3.1, to prove that the Cayley graph G_i of Z_n with respect to S_i is $|S_i|$-connected for all i. This holds for $i = m$, by the result in [2], pp. 47-49 mentioned in the previous proof. It also holds for $i = 1$, by Lemma 4.2. For any other value of i, note that since n is odd and $2t_i \leq (n-1)/3$, it follows that $S_i \cup \{0\}$ contains at least $n/3$ consecutive elements and hence intersects every coset of every nontrivial subgroup of Z_n. Let $A \subset Z_n$ be an arbitrary set of vertices of G_i and put $B = S_i \cup \{0\}$. Note that $(A + B) \setminus A$ is the set of all neighbors of A in G_i that lie outside A and hence if $A + B = Z_n$ then A cannot be separated from any nonempty subset of the graph (by deleting vertices outside A). Otherwise, define $H = \{x \in Z_n : x + A + B = A + B\}$

and note that H is a subgroup of Z_n. Since B intersects every coset of every nontrivial subgroup of Z_n, and as $A+B+H=A+B$ is a union of cosets of H and $A+B$ is not the whole group, it follows that $H=\{0\}$ is the trivial subgroup. Thus, by Kneser's Theorem,

$$|(A+B)\setminus A|\geq|A+H|+|B+H|-|H|-|A|=|A|+|B|-1-|A|=|S_i|.$$

It follows that A cannot be separated from any nonempty subset of vertices by deleting less than $|S_i|$ vertices, implying that G_i is $|S_i|$ connected, and completing the proof. $\Box$

The final ingredients in the proof of Theorem 1.1 are the following.

Lemma 4.6 *Let $V=Z_{2q-1}\cup\{v\}$ be a set of $2q$ vertices. For each $i\in Z_{2q-1}$, let M_i denote the perfect matching consisting of all edges ab where $a,b\in Z_{2q-1}$ are distinct and $a+b=i$ (with addition taken modulo $2q-1$) and one additional edge connecting v to $i/2$ (division computed in Z_{2q-1}.) Suppose $k\geq 2$, and let G_k denote the graph on V whose edges are all edges of $M_0\cup M_1\cup\ldots\cup M_{k-1}$. Then G_k is k-connected.*

Proof: Note that the neighbors of v in Z_{2q-1} consist of two arcs: $0,1,\ldots,\lfloor(k-1)/2\rfloor$ and $q,q+1,\ldots,q+\lfloor(k-2)/2\rfloor$.

Suppose that a set T of $k-1$ vertices separates G_k into two parts with classes of vertices S' and S''. Obviously, T cannot separate v from the rest of the vertices (since v has degree k). Hence there exist vertices $i\in S'$, $i+1,\ldots,i+t-1\in T$, and $i+t\in S''$ $(t\geq 1)$. Obviously, i and $i+t$ cannot be adjacent, hence

$$i+(i+t)=2i+t\not\equiv 0,1,\ldots,k-1 \pmod{2q-1}. \tag{5}$$

The vertices i and $i+t$ have $k-t$ common neighbors: the vertices $-i,-i+1,\ldots,-i+k-t-1$, and clearly these must be in T. Moreover, these vertices are different from $i,i+1,\ldots,i+t$. Indeed, if $-i+s=i+r$ for some $0\leq s\leq k-t-1$, $0\leq r\leq t$, then $2i+t=s-r+t\in\{0,\ldots,k-1\}$, contradicting (5).

Thus T contains $i+1,\ldots,i+t-1$ as well as $-i,-i+1,\ldots,-i+k-t-1$. These are $(t-1)+(k-t)=k-1$ vertices, and so T cannot contain any other ones. Since every pair of consecutive non-adjacent vertices $j,j+1$ have $k-1$ common neighbors $-j,-j+1,\ldots,-j+k-2$, it follows that if $j,j+1$ are not in T, then either both of them are in S' or both are in S''. Therefore, the vertices in $V-(T\cup\{v\})$ form two arcs along the cycle Z_{2q-1}, the sets $A'=\{-i+k-t,-i+k-t+1,\ldots,i\}\subseteq S'$ and $A''=\{i+t,i+t+1,\ldots,-i-1\}\subseteq S''$.

To conclude, it suffices to show that the set of neighbors of v contains a member of S' as well as a member of S'', contradicting the assumption that T separates S' and S''. Interchanging the roles of $-i$ and $i+1$ if necessary, we may assume that $0\leq i\leq q-1$.

First, consider the set A'. Vertex 0 is a neighbor of v and it is in A' unless $-i+k-t>0$; in this latter case $-i+k-t\in A'$ is a neighbor of v unless $-i+k-t>\lfloor(k-1)/2\rfloor$. But this last inequality implies that $0\leq 2i+t\leq 2\lfloor k/2\rfloor-t\leq k-1$, contradicting (5).

Second, consider A''. Vertex q is a neighbor of v and it is in A'' unless $i+t>q$; in this latter case $i+t\in A''$ is a neighbor of v unless $i+t>q+\lfloor(k-2)/2\rfloor$, which implies that $2i+t\geq 2q+2\lfloor k/2\rfloor-t\geq 2q-1$.

On the other hand, we have $2i+t \leq 2(q-1)+k = (2q-1)+(k-1)$. This contradicts (5), and completes the proof. $\Box$

Corollary 4.7 *For every* $m > 2$ *and every sequence of integers* $k_1, k_2, \ldots, k_m \geq 2$ *such that* $n = 1 + \sum_{i=1}^{m}(k_i - 1)$ *is even,*

$$f_m(k_1, \ldots, k_m) = n.$$

Proof : Define $z_0 = 0$, $z_i = \sum_{j=1}^{i}(k_i - 1)$ and consider the coloring of the complete graph on $Z_{2q-1} \cup \{v\}$ in which color class number i consists of all edges in the matchings $\cup_{j=z_{i-1}}^{z_i} M_j$. Since each of the graphs consisting of all edges except those of a fixed color is a union of consecutive matchings, its connectivity equals its degree of regularity, by the last lemma. The result thus follows from Theorem 3.1. $\Box$

Proof of Theorem 1.1: The fact that for all $k_1, \ldots, k_m$ that satisfy (i) or (ii), $f_m(k_1, \ldots, k_m) > 1 + \sum_{i=1}^{m}(k_i - 1)$ follows from Corollary 4.1. The main part of the theorem follows from Theorem 4.3, Lemma 4.5 and Corollary 4.7. $\Box$

5 Concluding remarks

- The construction described in Section 2 provides the value of $f_2(k, k) = 2k - 1$ for $k = (p+1)/2$, where $p \equiv 1 (\text{mod } 4)$ is a prime. This follows from Theorem 1.1 as well as from Theorem 4.3 or Lemma 4.5, and in fact the graphs corresponding to this construction are the Paley graphs, which are Cayley graphs of Z_p with respect to all quadratic non-residues. These graphs are self complementary.

- Lemma 4.5, for the special case in which $p = \sum_{i=1}^{m}(k_i - 1)$ is a prime, can be proved in a simpler way by a general construction, as it is easy to show, using the Cauchy-Davenport Theorem (see [3]), that the Cayley graph of Z_p with respect to **any** symmetric set S of generators, is $|S|$-connected.

- By the proof of Theorem 3.1 whenever $f_m(k_1, \ldots, k_m) = 1 + \sum_{i=1}^{m}(k_i - 1)$ then this can be demonstrated by real vectors, and there is no need to use the complex field.

- Our main result here characterizes all cases in which $f_m(k_1, \ldots, k_m) = 1 + \sum_{i=1}^{m}(k_i - 1)$. The problem of determining the precise value of $f_m(k_1, \ldots, k_m)$ for all admissible values of $m, k_1, \ldots, k_m$ seems difficult and remains open, and so does the more general problem of characterizing all sequences of integers $k_1, k_2, \ldots, k_m, n$ such that there is an UPB of size n in $C^{k_1} \otimes \ldots \otimes C^{k_m}$.

References

[1] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin and B. M. Terhal, Unextendible product bases and bound entanglement, Phys. Rev. Lett. 82, 5385 (1999).

[2] J. A. Bondy and U.S. R. Murty, *Graph Theory with Applications*, Macmillan Press, London, 1976.

[3] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* 10 (1935), 30–32.

[4] H. Davenport, *Multiplicative Number Theory,* Second Edition, revised by H.L. Montgomery, Springer Verlag, Berlin, 1980.

[5] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin and B. M. Terhal, Unextendible product bases, uncompletable product bases and bound entanglement, to appear.

[6] L. Lovász, On the Shannon capacity of a graph, IEEE Trans. Inform. Theory **25** (1979), 1–7.

[7] L. Lovász, M. Saks and A. Schrijver, Orthogonal representations and connectivity of graphs, Linear Algebra Appl. 114/115 (1989), 439–454.

[8] L. Lovász, M. Saks and A. Schrijver, A correction: orthogonal representations and connectivity of graphs, to appear

[9] H.B. Mann, *Addition theorems : The addition theorems of group theory and number theory*, Interscience, New York, 1965.

[10] M. Newman, On a theorem of Čebotarev, Linear and Multilinear Algebra 3 (1975/6), 259-262.

[11] R. Stanley, *Enumerative combinatorics, Vol. 2*, Cambridge Studies in Advanced Mathematics, 62, Cambridge University Press, Cambridge, 1999.