1 Introduction

In these notes, we focus on the even cycle problem: determining the maximum number of edges in an \( n \)-vertex graph that does not contain a certain list of even cycles. In the previous sections we gave constructions showing \( \text{ex}(n, C_{2k}) = \Omega(n^{1+1/k}) \) for \( k \in \{2, 3, 5\} \). In this section, we give the proof of the Even Cycle Theorem of Bondy and Simonovits [3] (also attributed to Erdős):

**Theorem 1.** For \( k \geq 2 \), \( \text{ex}(n, C_{2k}) = O(n^{1+1/k}) \).

The upper bound in this theorem is conjectured to be tight up to a constant factor by Erdős and Simonovits [7]. We arrive at this theorem via a detour to another extremal problem, namely that of finding cycles of length \( \ell \) mod \( k \) in a graph. This approach is due to the author [19].

1.1 Cycles mod \( k \)

For \( k \geq 2 \) and \( \ell \geq 0 \), let \( \mathcal{C}(k, \ell) \) denote the family of all cycles of length \( \ell \) modulo \( k \), and \( \mathcal{C}(k) := \mathcal{C}(\ell, 0) \). In proving the Even Cycle Theorem, we determine almost tight bounds on \( \text{ex}(n, \mathcal{C}(k, \ell)) \) as well as a method for giving upper bounds on \( \text{ex}(n, \mathcal{C}) \) for various other infinite families of cycles. Bollobás [2] was the first to show that \( \text{ex}(n, \mathcal{C}(k, \ell)) \) is linear in \( n \) for each pair \( (k, \ell) \) such that \( \mathcal{C}(k, \ell) \) contains even cycles, by showing

\[
\text{ex}(n, \mathcal{C}(k, \ell)) \leq \frac{1}{k}[(k + 1)^k - 1]n.
\]
This has been successively improved by many authors [18]. We shall prove the following result:

**Theorem 2.** Let \((k, \ell)\) be a pair of positive integers such that \(k\) is odd or \(\ell\) is even. Then \(\text{ex}(n, \mathcal{C}(k, \ell)) < 4kn\).

An \(n\)-vertex graph whose blocks are all cliques of order \(k - 1\) contains no cycle of length zero modulo \(k\), so for all \(k\), \(\text{ex}(n, \mathcal{C}(k)) \geq \frac{1}{2}(k - 1)(n - 1)\) for infinitely many \(n\). If \(k\) is odd, then \(K_{k-1, n-k+1}\) contains no cycle of length 0 mod \(k\) and so \(\text{ex}(n, \mathcal{C}(k)) \geq (k - 1)(n - k + 1)\). This shows Theorem 2 is tight up to a factor of roughly 2.

**Conjecture 3.** The extremal graphs for \(\mathcal{C}(k)\) are graphs whose blocks are all cliques of order \(k - 1\) if \(k\) is even, and \(K_{k-1, n-k+1}\) if \(k\) is odd.

It is an exercise to verify that this conjecture is true when \(k = 2\). Using his subdivided grid theorem for graphs of large tree-width, Thomassen [18] gave a polynomial-time algorithm for finding a cycle of length 0 mod \(k\) in a graph or a certificate that no such cycle exists. It is an open question as to whether such an algorithm exists for finding a cycle of length \(\ell\) mod \(k\) when \(\ell \neq 0\). Recent results of the author [20] improve Theorem 2 as follows:

**Theorem 4.** Let \(k \geq 2\) and \(\ell \geq 0\) be even with \(\ell < k\). Then

\[
\text{ex}(n, \mathcal{C}(k, \ell)) = \Theta(n^{\text{ex}(k, C_{\ell})}).
\]

In particular,

\[
\text{ex}(n, \mathcal{C}(k, \ell)) \leq 8\ell k^{2/\ell} n.
\]

For \(\ell = \Omega(\log k)\), this gives \(\text{ex}(n, \mathcal{C}(k, \ell)) = O(\ell n)\), which is a substantial improvement for small \(\ell\) over the bound from Theorem 5 and sharp up to a constant since \(K_{\ell/2-1, n-\ell/2+1}\) contains no cycle of length \(\ell\) mod \(k\). Furthermore, for \(\ell \in \{4, 6, 10\}\), \(\text{ex}(n, \mathcal{C}(k, \ell)) = \Theta(k^{2/\ell} n)\) due to the existence of Moore graphs of girth \(\ell + 2\) and at most \(k + \ell - 1\) vertices.

### 1.2 Breadth first search trees

We require some terminology. If \(v\) is a vertex of a connected graph \(G\), then a *breadth first search tree* rooted at \(v\) is a spanning tree \(T\) of \(G\) created as follows. Having found
a tree $T_i \subseteq G$ with vertices $v = v_0, v_1, v_2, \ldots, v_i$, we pick a vertex $v_{i+1} \in V(G) \setminus V(T_i)$ such that $d_G(v, v_{i+1})$ is a minimum, and then let $V(T_{i+1}) = V(T_i) \cup \{v_{i+1}\}$ and select a vertex $v_j \in V(T_i)$ such that $\{v_j, v_{i+1}\} \in E(G)$ and $j$ is a minimum, and set $E(T_{i+1}) = E(T_i) \cup \{v_j, v_{i+1}\}$. If $T$ is a breadth first search tree in $G$, rooted at $v$, then $d_G(v, w) = d_T(v, w)$ for all $w \in V(G)$ – in other words $T$ preserves the distance from $v$ in $G$. In particular, the $i$th level of $T$ is $L_i(T) = \{w \in V(G) : d_G(v, w) = i\}$. The height of $T$ is $\max\{d_T(v, w) : w \in V(T)\}$. Note that the edges of $G$ lie either between two consecutive levels of $T$, or inside levels of $T$. The radius of a graph $G$ is the minimum $r$ such that there exists a vertex $v \in V(G)$ for which $d_G(u, v) \leq r$ for every $u \in V(G)$. Equivalently, the radius is the smallest possible height of any breadth first search tree in $G$.

1.3 Consecutive even cycle lengths

In this section, we use the methods of [19] to prove the following theorem, which implies Theorem 2.

**Theorem 5.** Let $k \geq 2$, and let $G$ be a bipartite graph of average at least $4k$ and radius $r$. Then $G$ contains cycles $C_{2m}, C_{2m+2}, \ldots, C_{2m+2k-2}$ for some $m \leq r$.

The complete bipartite graph $K_{k, n-k+2}$ does not contain cycles of $k$ consecutive even lengths, so Theorem 5 is best possible up to a factor 2. We now prepare for the proof. The following lemma is required. Here a $\theta$-graph consists of a cycle plus an additional edge joining two nonconsecutive vertices on the cycle.

**Lemma 6.** Let $G$ be a $\theta$-graph with $n$ vertices and suppose $V(G) = A \cup B$ where $A, B$ are non-empty. Then for every $\ell < n$, $G$ contains a path of length $\ell$ with one end in $A$ and one end in $B$, unless $G$ is bipartite with parts $A$ and $B$.

This lemma is left as an exercise. The purpose of the additional edge $e$ in a $\theta$-graph is to break the possibility that the vertices of $A$ are every $m$th vertex along the cycle $G - e$ for some $m|n$, for in that case, there is no path of length zero mod $m$ with one end in $A$ and one end in $B$. The second lemma we need follows from a longest path argument:

**Lemma 7.** If $k \geq 3$ and $F$ is a bipartite graph of minimum degree at least $k$, then $F$ contains a $\theta$-graph with at least $2k$ vertices.
Lemma 7 is best possible since $K_{k-1,n-k+1}$ does not contain even a cycle with $2k$ vertices.

**Proof of Theorem 5.** We start with a bipartite graph $G$ of radius $r$ and average degree at least $4k$. Let $T$ be a breadth first search tree in $G$. Then

$$e(G) = \sum_{i=1}^{r} e(L_{i-1}(T), L_i(T)).$$

Since

$$|V(G)| = \sum_{i=0}^{r} |L_i(T)|$$

we gather that for some $i \leq r$, the edges of $G$ with one end in $L_{i-1}(T)$ and the other end in $L_i(T)$ form a bipartite graph $F$ of average degree at least $2k$. Then $F$ has a subgraph of minimum degree at least $k+1$, so by Lemma 7, $F$ contains a $\theta$-graph $F'$ with at least $2k+2$ vertices. Let $U = V(F') \cap L_{i-1}(T)$ and $V = V(F') \cap L_i(T)$. Let $T'$ be the minimum subtree of $T$ such that $V(T') \cap U = V(F') \cap U$. Then the vertex $u$ of $T'$ closest to the root of $T$ has degree at least two in $T'$. This implies $T' - \{u\}$ has at least two components. Let $A$ be the set of vertices of $U$ in one of the components, and $B = V(F') \setminus A$. Then $V(F') = A \cup B$, but $A$ and $B$ do not form the bipartition of $F'$. By Lemma 6, for each $\ell \in \{1, 2, \ldots, k\}$, there exists a path $P$ of length $2\ell$ in $F'$ with one end $a \in A$ and one end $b \in B$. Since $P$ has even length $b \in V(T') \cap L_{i-1}(T)$. Let $m - 1$ denote the height of $T'$, and note $m - 1 \leq r - 1$. Then $a, b \in V(T')$ are connected in $T'$ by a unique path of length $2m - 2$, since they are in different branches of $T'$. Together with $P$, this path forms a cycle of length $2m - 2 + 2\ell$ in $G$, and this works for any $\ell \in \{1, 2, \ldots, k\}$, as required. \qed

1.4 Proof of Theorem 1

To prove Theorem 1, we show specifically that

$$\text{ex}(n, C_{2k}) \leq 8(k - 1)n^{1+1/k}$$

from Theorem 5. Let $G$ be a graph with at least $8(k - 1)n^{1+1/k}$ edges on $n \geq 8(k - 1)$ vertices. Pass to a bipartite subgraph with at least $4(k - 1)n^{1+1/k}$ edges. Let $H$ be a component of the $d$-core of this subgraph, where $d = 4(k - 1)n^{1/k}$. If $T$ is a breadth first search tree in $H$, and $U_r = \bigcup_{i=0}^{r} L_i(T)$, we claim $H[U_r]$ has average degree at least $4(k - 1)$ for some $r \leq k$. For some smallest $r \leq k$, we have
\[ |L_r(T)| \leq n^{1/k}|L_{r-1}(T)|. \] Then \( H[U_r] \) has at least \( d|L_{r-1}(T)| \geq 4(k-1)|L_r(T)| \) edges. Since \( |L_{j-1}(T)| \leq n^{-1/k}|L_j(T)| \) for all \( j < r, \) and \( n \geq 8(k-1), \)

\[ |U_r| = \sum_{j=0}^{r} |L_j(T)| \leq |L_r(T)| \sum_{j=0}^{r} n^{-j/k} < 2|L_r(T)|, \]

\( H[U_r] \) has average degree at least \( 4(k-1). \) By Theorem 5, \( H[U_r] \) contains cycles \( C_{2m}, C_{2m+2}, \ldots, C_{2m+2k-4} \) where \( 2 \leq m \leq 2r. \) In particular, \( C_{2k} \) is amongst those cycles, and so \( C_{2k} \subseteq G. \)

By refining the above proof, Pikhurko [14] showed \( \text{ex}(n, C_{2k}) < (k-1)n^{1+1/k}, \) and recently Bukh and Jiang [5] showed \( \text{ex}(n, C_{2k}) < 80\sqrt{k \log k} \cdot n^{1+1/k} + O(n). \) It is an open problem to determine whether \( \text{ex}(n, C_{2k}) < cn^{1+1/k} \) for some absolute constant \( c.\)

\section{Cycles in hypergraphs}

Recall a \( k \)-cycle is a hypergraph \( C_k \) consisting of edges \( e_0, e_1, \ldots, e_{k-1} \) such that the sets \( e_i \cap e_{i+1} \) with subscripts mod \( k \) have a system of distinct representatives – in other words, there are distinct vertices \( v_i \in e_i \cap e_{i+1} \) for all \( i \) (subscripts mod \( k \)).

\subsection{Excluding a 2k-cycle}

The following extension of Theorem 1 was proved by Győri and Lemons [9]:

\textbf{Theorem 8.} For all \( r \geq 3 \) and \( k \geq 1, \) \( \text{ex}_r(n, C_{2k}) = O(n^{1+1/k}) \) and \( \text{ex}_r(n, C_{2k+1}) = O(n^{1+1/k}). \)

It is somewhat surprising that the upper bound here for \( \text{ex}_r(n, C_{2k}) \) is the same as for \( \text{ex}_r(n, C_{2k+1}), \) since for \( r = 2 \) and \( k \geq 2, \) \( \text{ex}_2(n, C_{2k}) = O(n^{1+1/k}) \) by Theorem 1, whereas by the Simonovits color-critical theorem, for \( k \geq 1, \) \( \text{ex}_2(n, C_{2k+1}) = \lfloor n^2/4 \rfloor \) if \( n \) is large enough. Theorem 8 is equivalent to a statement about \( m \times n \) bipartite graphs without short cycles. Namely, if \( H \) is an \( r \)-uniform hypergraph with \( m \) edges, \( n \) vertices, and no \( C_k, \) then the bigraph of \( H \) is an \( m \times n \) bipartite graph which does not contain \( C_{2k}, \) and where every vertex in the part of size \( m \) has degree exactly \( r. \) The Zarankiewicz numbers \( z(m, n, C_{2k}) \) describe the maximum number of edges
such a graph may have, and upper bounds on them were given by Naor and the author [12]:

**Theorem 9.** Let \( k \geq 2 \). Then

\[
\begin{align*}
z(m, n, C_{2k}) \leq \begin{cases} 
(2k - 3)[m^{1/2}n^{1/2+1/k} + m + n] & \text{if } k \text{ is even} \\
(2k - 3)[(nm)^{1/2+1/2k} + m + n] & \text{if } k \text{ is odd}
\end{cases}
\]

The proof of Theorem 9 is modeled on the proof of Theorem 1 given in preceding sections. Theorem 8 for large \( r \) follows immediately from Theorem 9: if \( H \) is an \( r \)-uniform \( C_k \)-free \( n \)-vertex hypergraph with \( m \) edges, then \( z(m, n, C_{2k}) \geq rm \). If \( r > 4k - 3 \), then applying Theorem 9 we obtain the bounds in Theorem 8.

### 2.2 Moore bound for hypergraphs

Let \( \mathcal{C}_g = \{C_2, C_3, \ldots, C_g\} \). The girth of a hypergraph containing a cycle is the length of a shortest cycle. One can obtain a Moore bound for \( r \)-graphs: if \( H \) is a \( (d + 1) \)-regular \( n \)-vertex \( r \)-graph of girth \( 2g + 1 \geq 3 \), then by counting the number of vertices at distance at most \( g \) from any vertex we find

\[
n \geq 1 + (r - 1)d + \cdots + (r - 1)^g d^g.
\]

A similar bound works when the girth is \( 2g + 2 \). In fact, the argument of non-backtracking walks works when \( H \) has average degree \( d + 1 \geq 2 \), and so

\[
\text{ex}_r(n, \mathcal{C}_{2g}) \lesssim \frac{1}{r(r - 1)} n^{1+1/g}
\]

and also for \( g \geq 1 \),

\[
\text{ex}_r(n, \mathcal{C}_{2g+1}) \lesssim \frac{1}{r} \left(\frac{n}{r}\right)^{1+1/g}.
\]

For girth three – linear hypergraphs – the upper bound is \( \binom{n}{2}/(\binom{r}{2}) \), which is the number of edges in a 2-design. For girth four, the problem has greater depth, and the following was proved by Ruzsa and Szemerédi [16]:

**Theorem 10.** *(Ruzsa-Szemerédi Theorem)* For all \( r \geq 3 \), \( \text{ex}_r(n, \mathcal{C}_3) = o(n^2) \).

The proof uses Szemerédi’s Regularity Lemma, which we visit later. This theorem is related to the problem of determining the maximum size of a set \( A \subseteq \mathbb{N} \) with no three-term arithmetic progression, to which we return shortly. For girth five, the following was proved by Lazebnik and the author [11]:
Theorem 11. \( \text{ex}_3(n, \mathcal{C}_4) \sim \frac{1}{6} n^{3/2} \).

The construction is very simple: we take the triangles of the Erdős-Rényi orthogonal polarity graph with \( q^2 + q + 1 \) vertices, of which there are exactly \( \binom{q+1}{3} \). It is an open question to determine the order of magnitude of \( \text{ex}_4(n, \mathcal{C}_4) \), in particular, Lazebnik and the author [11] conjecture \( \text{ex}_r(n, \mathcal{C}_4) = \Theta(n^{3/2}) \) for all \( r \geq 2 \), and show

\[
\text{ex}_r(n, \mathcal{C}_4) = \Omega(n^{3/2} \exp(-c_r \sqrt{\log n})
\]

using a construction of Behrend [1]. The order of magnitude of \( \text{ex}_r(n, \mathcal{C}_g) \) is not known when \( r \geq 3 \) and \( g \geq 5 \).

3 Applications

Here we give some indications of applications to various other areas of mathematics and computer science.

3.1 Arithmetic progressions

Let \( A \subset [N] \) have no three-term arithmetic progression. We show how to build a 3-graph \( H_A \) with \( \Theta(N) \) vertices such that \( H \) has no \( C_2 \) and no \( C_3 \) and \( O(|A| N) \) edges. The parts of \( H_A \) are \( X_i = [iN] \) for \( 1 \leq i \leq 3 \), and the edges of \( H_A \) are the sets \( \{x, x + a, x + 2a\} \) for \( a \in A \). Then \( e(H_A) = |A| N \), and we claim \( H_A \) is \( C_2 \)-free and \( C_3 \)-free. If \( H = H_A \) contains a 2-cycle, then there are edges \( \{x, x + a, x + 2a\} \) and \( \{y, y + b, y + 2b\} \) of \( H \) intersecting in two vertices \( x + ia = y + ib \) and \( x + ja = y + jb \) where \( i \neq j \), however this implies \( x = y \) and \( a = b \), so the edges are identical. If \( H \) contains a 3-cycle with edges \( e_x = \{x, x + a, x + 2a\}, \quad e_y = \{y, y + b, y + 2b\} \) and \( e_z = \{z, z + c, z + 2c\} \), where \( a, b, c \in A \), then by symmetry we may assume \( e_x \cap e_y = \{x\} = \{y\} \), \( e_y \cap e_z = \{y + b\} = \{z + c\} \), and \( e_z \cap e_x = \{x + 2a\} = \{z + 2c\} \). It follows that \( x = y, x - z = c - b \) and \( x - z = 2(c - a) \). Therefore \( c - b = 2(a - c) \) which means \( b + c = 2a \). By choice of \( A \), we must have \( a = b = c \) and then \( x = y = z \), a contradiction. Therefore \( H \) is \( C_3 \)-free.

The Ruzsa-Szemerédi Theorem states \( \text{ex}_3(n, \mathcal{C}_3) = o(n^2) \). Since we just showed \( \text{ex}_3(n, \mathcal{C}_3) = \Omega(n|A|) \) when \( A \subset [n] \) has no three term progression, we gather \( |A| = o(n) \). In other words, any set of integers not containing an arithmetic progression of
length three has zero density. This is Roth’s Theorem [15]. The current best upper bound on the size of a subset of $[n]$ with no arithmetic progression of length three is of order $n/(\log n)^{1-o(1)}$, due to Sanders [17]. On the other hand, we present a construction of a set of size $n \exp(-O(\sqrt{\log n}))$ which has no three term progressions, due to Behrend [1], and summarising we get

$$\frac{n}{\exp(\Omega(\sqrt{\log n}))} \leq \exp_3(n, C_3) \leq \frac{n}{(\log n)^{1-o(1)}}$$

For the Behrend construction, let $S_{d, R}$ denote the set of $x \in \mathbb{R}^d$ such that

$$dR^2/64 \leq x_1^2 + x_2^2 + \cdots + x_d^2 \leq dR^2/16.$$

Consider the set $S$ of points $(x_1, x_2, \ldots, x_d)$ in $S_{d, R}$ such that $R/8 \leq x_i < R/4$ and $x_i$ is an integer for all $i \leq d$. Now $|S| \geq (R/8)^d$. Therefore there exists $R_0 : \sqrt{d}R/8 \leq R_0 \leq \sqrt{d}R_0/2$ such that the number of solutions to $x_1^2 + x_2^2 + \cdots + x_d^2 = R_0^2$ with $x_i < R/4$ and $x_i$ a non-negative integer is at least

$$|S| \cdot \frac{R}{dR} \geq d^{-1} R^{d-1} 8^{-d}.$$ 

Let $S_0$ be this set of $x \in S$: with $\|x\| = R_0$ and $x_i < R/4$ for $1 \leq i \leq d$. Let $\phi : S_0 \to \mathbb{N}$ be defined by

$$\phi(x) = \sum_{i=1}^d x_i R_i^{-1}.$$ 

In other words, $\phi$ translates a point in $S_0$ to its corresponding integer in $R$-adic representation. Let $A = \{\phi(x) : x \in S_0\}$ and note $A \subset [N]$ where $N = R^{d+1}$. If $\phi(x) + \phi(y) = 2\phi(z)$ then since $x_i, y_i, z_i < R/4$, $x_i + y_i = 2z_i$ in the integers, for $1 \leq i \leq d$. This implies the vector equation $x + y = 2z$ in $S_0$. The convexity of $S_{d, R}$ shows that $x = y = z$: taking norms we get

$$\|x\|^2 + \|y\|^2 + 2\|x\|\|y\| \cos \theta = 4\|z\|^2$$

where $\theta$ is the angle between $x$ and $y$. Since $\|x\| = \|y\| = \|z\| = R_0$, $\theta = 0$ and so $x = y = z$. Since $\phi$ is injective, $|A| = |S_0|$. We obtain

$$|A| \geq \frac{R^{d-1}}{d \cdot 8^d} \geq \frac{N}{d R^{2d}}.$$ 

Select $R = \exp(\sqrt{\log N})$ and $d = \sqrt{\log N}$ (we lose little in assuming these are integers) so that

$$|A| \geq \frac{N}{\exp(O(\sqrt{\log N}))}.$$
This completes the construction.

We remark that as hypergraph triangles correspond to three-term progressions, there are other hypergraph configurations which give longer arithmetic progressions. Specifically, the hypergraph $F$ with edges $\{1, 2, 3\}, \{1, 4, 5\}, \{3, 4, 6\}$ and $\{2, 5, 7\}$ corresponds to four-term arithmetic progressions. The following is a notorious conjecture of Brown, Erdős and Sós [4]:

Conjecture 12. Let $H$ be an $n$-vertex linear 3-graph not containing $F$. Then $e(H) = o(n^2)$.

3.2 Codes and linear dependencies

A $q$-ary code is a subset of $\mathbb{F}_q^n$. The minimum distance of a code $C$ is $\delta(C) = \min\{d_H(u, v) : u, v \in C\}$ where $d_H(\cdot, \cdot)$ is the standard Hamming distance. If $C$ is a subspace of $\mathbb{F}_2^n$, then $C$ is linear and clearly $\delta(C) = \min\{d_H(u, 0) : u \in C\}$. In coding theory an important problem is to construct small codes with large minimum distance. This is due to the fact that a code with minimum distance $2t + 1$ is a $t$-error-correcting code. In other words, if a codeword $u \in C$ is sent across a noisy channel which corrupts at most $t$ bits of $u$, then $u$ can be recovered uniquely from the corrupted codeword received. Given a linear code $C \subset \mathbb{F}_2^m$ with dimension $\ell$, an $m - \ell$ by $m$ matrix $A$ is called a parity check matrix for $C$ if $C$ is the nullspace of $A$. The matrix $A$ is $r$-sparse if every column of $A$ has at most $r$ non-zero entries. If a corrupted codeword $z$ is received, then one computes the vector $x$ of minimum Hamming weight such that $Ax = Az$, and then decode $z$ to $z - x$. The number of errors corrected is $t$ if $C$ has minimum distance $2t + 1$, or equivalently no $2t$ columns of $A$ are linearly dependent. As such computations are faster if the sparseness of $A$ is exploited, it is desirable to obtain codes with sparse parity check matrices. Indeed, sparse parity check matrices occur in many of the known constructions of codes. Let $B_q(r)$ denote the Hamming Ball of radius $r$ in $\mathbb{F}_q^n$, the set of all vectors of weight at most $r$.

Theorem 13. Let $X \subset \mathbb{F}_q^n$ be a set of vectors of Hamming weight $r \geq 2$, and suppose that there is no linear dependency of exactly $2k$ vectors in $X$. Then for some constant $c \leq 2$, $|X| = O(|B_q(r)|^{1/2 + c/k}).$

Proof. The proof for $r$ odd is complex [13], so we only give the proof for $r$ even, say
\( r = 2s \), and we use \( c = 1/2 \). We decompose each \( x \in X \) into two vectors \( x(0) \) and \( x(1) \) such that \( x(0) \oplus x(1) = x \) and \( x(0), x(1) \) both have Hamming weight \( s \). Form the graph \( G \) whose vertex set comprises all vectors in \( \mathbb{F}_q^n \) of Hamming weight \( s \), and where two vectors \( y, z \) form an edge if there exists \( x \in X \) such that \( x(0) = y \) and \( x(1) = z \). Then \( |V(G)| = |\mathbb{B}_q(s)| \) and \( |E(G)| = |X| \). Suppose \( G \) contains a cycle of length \( 2k \), with edges \( \{y_i, y_{i+1}\} \) for \( 0 \leq i \leq 2k - 1 \) with subscripts mod \( 2k \). Then trivially

\[
(y_0 + y_1) + (y_2 + y_3) + \cdots + (y_{2k-2} + y_{2k-1}) = (y_1 + y_2) + (y_3 + y_4) + \cdots + (y_{2k-1} + y_0)
\]

which means by definition of \( G \) that the vectors \( x_i = y_{2i} + y_{2i+1} \) and \( z_i = y_{2i+1} + y_{2i+2} \) for \( 0 \leq i < k \) have the same sum:

\[
x_0 + x_1 + \cdots + x_{k-1} = z_0 + z_1 + \cdots + z_{k-1}.
\]

This a linear dependency of size \( 2k \), so we conclude \( G \) contains no cycle of length \( 2k \). By Theorem 1, \(|X| = e(G) \leq |\mathbb{B}_q(s)|^{1+1/k} = O(|\mathbb{B}_q(r)|^{1/2+1/2k})\). \( \square \)

The main point in this theorem is that the cycle \( C_{2k} \) in the auxiliary graph \( G \) gives a field-independent linear dependency of \( 2k \) vectors. It is also not hard to show that for a linear dependency of \( k \) vectors over \( \mathbb{F}_2^n \), when \( k \) is odd, \( \Theta(n^r) \) vectors may be necessary.

A set of vectors is \( k \)-wise independent if no set of at most \( k \) of the vectors is linearly dependent. The theorem above in particular says that if \( X \) is \( 2k \)-wise independent, where \( 2k = \frac{r}{5} \), then \(|X| = O(n^{r/2+\delta}) \). In fact, this is almost tight due to random sets of vectors:

**Theorem 14.** Let \( X \) be a set of vectors in \( \mathbb{F}_q^n \), chosen uniformly and independently from \( \mathbb{B}_q(r) \) with probability \( p = n^{-r/2} \). Then with positive probability, \(|X| = \Omega(n^{r/2+\delta}) \) and \( X \) is \( \frac{r}{28} \)-wise independent.

It is a challenging problem to construct explicitly a set of \( \Theta(n^2) \) vectors in \( \mathbb{F}_q^n \) of weight four such that no set of \( O(\log n) \) of the vectors are linearly independent. Finally we mention the conjecture of Feige [8]:

**Conjecture 15.** Let \( r \geq 2 \) and \( \log n \leq k \leq n \). Then there is a constant \( c = c(r) \) such that if \( X \subset \mathbb{F}_2^n \) is a \( k \)-wise independent set of vectors of weight \( r \),

\[
|X| \leq (\log n)^c n^{r/2} k^{1-r/2}.
\]
The conjecture is clearly true when \( r = 2 \), since a graph of girth at least \( \log n \) has \( O(n) \) edges, by the Moore bound. For general \( r \), the conjecture, if true, is almost tight by a construction of random sets of vectors.

### 3.3 A little geometry

The following theorem due to Hoory [10] generalizes the Moore bound to \( m \times n \) bipartite graphs:

**Theorem 16.** Let \( G \) be an \( m \times n \) bipartite graph such that the average degree in the part of size \( m \) is \( d_m + 1 \geq 2 \) and the average degree in the part of size \( n \) is \( d_n + 1 \geq 2 \). If \( G \) has girth \( 2g + 2 \geq 4 \), then

\[
    n \geq \sum_{i=0}^{g} d_m \left\lceil \frac{i}{2} \right\rceil d_n \left\lfloor \frac{i}{2} \right\rfloor \quad \text{and} \quad m \geq \sum_{i=0}^{g} d_n \left\lceil \frac{i}{2} \right\rceil d_m \left\lfloor \frac{i}{2} \right\rfloor.
\]

In particular, for \( g \geq 2 \),

\[
    z(m, n, C_{2g}) \leq \begin{cases} 
    m^{1/2} n^{1/2+1/2g} + m + n & \text{if } g \text{ is even} \\
    (mn)^{1/2+1/2g} + m + n & \text{if } g \text{ is odd}
\end{cases}
\]

The bounds on Zarankiewicz number are along the lines of Theorem 9. As in the proof of the Moore Bound, the proof of this theorem is achieved by counting non-backtracking walks of length at most \( g \). We saw that Theorem 16 is tight when \( m = n \) and \( 2g + 2 \in \{6, 8, 12\} \). It is generally a very difficult problem to determine whether the theorem is tight for \( m < n \).

de Caen and Székely [6] showed that if \( P \) is a set of \( n \) points and \( L \) is a set of \( m \) lines in the Euclidean plane, then the number of the number of sequences \((p, L, q, M, r)\), where \( L, M \) are lines and \( p, q, r \) are points with \( p, q \in L \) and \( q, r \in M \), is \( O(mn) \), by applying Theorem 16 for \( g = 4 \). They make the following conjecture:

**Conjecture 17.** If \( P \) is a set of \( n \) points and \( L \) is a set of \( m \) lines in the Euclidean plane, then the number of triangles whose vertices are points in \( P \) and whose sides are segments of lines in \( L \) is \( O(mn) \).

This is equivalent to estimating the number of cycles of length six in the bipartite incidence graph of the points and the lines. Note that the conjecture is not true in the projective plane, since the number of triangles in a projective plane with \( m = n \) points and lines is asymptotic to \( \binom{n}{3} \).
References


