# On Sparse Parity Check Matrices

Hanno Lefmann* Pavel Pudlák† Petr Savický‡

November 3, 1999

**Abstract**

We consider the extremal problem to determine the maximal number $N(m,k,r)$ of columns of a 0-1-matrix with $m$ rows and at most $r$ ones in each column such that each $k$ columns are linearly independent modulo 2. For each fixed $k \geq 1$ and $r \geq 1$, we shall prove a probabilistic lower bound $N(m,k,r) = \Omega(m^{kr/2(k-1)})$; for $k$ a power of 2, we prove an upper bound $N(m,k,r) = O(m^{\lceil kr/(k-1)\rceil/2})$ which matches the lower bound for infinitely many values of $r$. We give some explicit constructions.

## 1 Introduction

We shall consider matrices $M$ over the two-element field $\mathbf{GF}_2$. If each $k$ column vectors of $M$ are linearly independent, we say that the columns are *$k$-wise independent*. By a *$(k,r)$-matrix* we mean a matrix, where the column vectors are $k$-wise independent and each column contains at most $r$ ones. We denote by $N(m,k,r)$ the maximal number of columns in a $(k,r)$-matrix with $m$ rows. The aim of this paper is to give estimates on the growth of the function $N(m,k,r)$. Matrices with $k$-wise independent columns are just parity check matrices for linear codes with minimal distance at least $k+1$. Thus our problem is to estimate sizes of sparse parity check matrices. We shall give lower and upper bounds on $N(m,k,r)$, which for infinitely many values of $k$ and $r$ match up to multiplicative constants. However, even for some small values, e.g. $k=4, r=4$, we still do not know the growth rate.

Some special cases of this problem and similar questions have been studied in combinatorics and graph theory. First let us note that we can consider a related problem where each column is required to have exactly $r$ ones. The extremal function for this problem has the same growth rate. Now this question can be stated as a problem about $r$-uniform hypergraphs. Namely, how many edges can an $r$-uniform hypergraph on $m$ vertices have so that it does not contain $l$ hyperedges, $1 \leq l \leq k$, which cover each vertex an even number of times? For $r=2$ we have ordinary graphs and the question is: how many edges can a graph on $m$ vertices have if its girth is at least $k+1$?

Though there are many papers on hypergraphs with forbidden configurations, apparently our question has not been studied for values $r > 2$. A related, but different, problem has been investigated by Calkin [Ca 95], who considered the question of how many random 0-1 vectors of length $m$ with exactly $r$ ones must be chosen to obtain a dependent set. Frankl and Füredi [FF 86] considered a problem, which is closely related to ours. They investigated three types of forbidden configurations of four hyperedges in $r$-uniform hypergraphs. They determined the growth rates for these types, and it turned out that these coincide. One of these types of forbidden configurations are four-tuples of hyperedges $E_1, E_2, E_3, E_4$ such that $E_1 \cup E_2 = E_3 \cup E_4$ and $E_1 \cap E_2 = E_3 \cap E_4$. These configurations are forbidden also if we assume 4-wise independence, however, not all linearly dependent four-tuples

*Universität Dortmund, FB Informatik, LS II, D-44221 Dortmund, Germany.
†Mathematical Institute, Academy of Sciences, Žitná 25, CZ 11567 Praha 1, Czech Republic.
‡Institute of Computer Science, Academy of Sciences, Prague, Czech Republic.

are of this type. We shall use an extension of their argument to prove an upper bound on $N(m,k,r)$. To prove a lower bound on $N(m,k,r)$, we utilize the probabilistic method.

Sparseness of a matrix is in general a useful property. For instance, several algorithms for matrix problems run faster on sparse matrices. A possible application of sparse parity check matrices is the following construction.

**Proposition 1.1** *Let $A$ be an $l \times m$ parity check matrix of a linear code of length $m$ with minimal distance at least $kr+1$, and let $B$ be a $(k,r)$-matrix with dimension $m \times n$. Then $A \times B$ is a parity check matrix of a code of length $n$ with minimal distance at least $k+1$.*

Just realize that the columns of $A \times B$ are sums of the columns of $A$. Namely, the $i$-th column $c$ of $A \times B$ is the sum of the columns of $A$ determined by the ones in the $i$-th column of $B$ i.e., $c$ is a sum of at most $r$ columns of $A$. As the columns of $A$ are $kr$-wise independent, each $k$ columns of $A \times B$ are independent.

This construction can be used to extend the length of a linear code, thus improving its rate, on the expense of reducing the minimal distance.
There are important application of parity check matrices in derandomization of probabilistic algorithms. They can be used to construct small sample spaces where variables preserve some independence. Namely, let $A$ be a parity check matrix of a linear code with minimal distance at least $d+1$. Let $A'$ be the dual code of $A$, i.e., the matrix whose rows are all rows of the space generated by the rows of $A$, each vector taken once. If we consider the columns as random 0-1 variables and rows as events, then the columns of $A'$ are $d$-wise independent.
Now suppose that $d = kr$ and let $B$ be a $(k,r)$-matrix. Then (in the same way as above) multiplying $A'$ by a matrix $B$ we get a matrix with $k$-wise independent columns. However, one can easily check that we do not need that $A'$ is constructed from a parity check matrix. Thus we have:

**Proposition 1.2** *Let $A$ be an $l \times m$ matrix with $kr$-wise independent columns (as random variables), and let $B$ be a $(k,r)$-matrix with dimension $m \times n$. Then $A \times B$ has $k$-wise independent columns.*

Let us note that Proposition 1.2 can be extended further to the case, where $A$ is only approximately $k$-wise independent ($(\varepsilon,k)$-biased in the sense of Alon, Goldreich, Håstad and Peralta [AGHP 92]), namely:

**Proposition 1.3** *Let $X = (X_1, ..., X_m)$ be an $(\varepsilon, kr)$-biased random vector, and let $B$ be a $(k,r)$-matrix of size $m$ by $n$. Then the vector $Y = X \times B = (Y_1, ..., Y_n)$ is $(\varepsilon, k)$-biased.*

For practical applications one would need explicit constructions of sparse parity check matrices, or at least efficient (say, polynomial time) algorithms for their construction. Also it seems that explicit constructions are necessary for finding good lower bounds on the function $N(m,k,r)$. It might be a difficult problem to construct explicitly matrices which match the upper bound. We do not know of such explicit constructions which match the upper bound except for $r = 2$ (i.e. graphs) and $k = 2,3,4,5,6,9,10$, and for $r = 3$ and $k = 4$. For fixed $k$ and $r$, a polynomial time algorithm can be produced from the probabilistic lower bound using the method of conditional probabilities. However, the exponent in the polynomial bound increases with $k$ and $r$, so for larger values it is not practical. Moreover, the algorithm does not give any insight into the structure of such matrices. Therefore we shall give three general explicit constructions of $(k,r)$-matrices with reasonably good parameters and one semi-explicit construction for $k = 4$.
Recently, Sipser and Spielman [SS 94, Spi 95] constructed asymptotically good codes using expander graphs. The parity check matrices of these codes are also sparse (each column and each row have only a constant number of nonzeros). One of the motivation for their research comes from the famous deep PCP theorem (namely that every set in $NP$ has polynomially checkable proofs), see [Spi 95d].

In the known proofs of this theorem efficient (but not asymptotically good) codes are constructed which have, among others, the following property. To determine if a word belongs to the code with high probability, we need to sample only a constant number of bits of the word. A direct construction of such codes is not known, but parity check matrices with a constant number of nonzeros in each row, which they constructed, are a step towards this goal. Let us note that Sipser and Spielman considered asymptotically good codes, while we consider only constant minimal distance, so our and their results are incomparable. Nevertheless, it shows that the question of sparse parity check matrices should be investigated in general.

## 2 A Probabilistic Lower Bound

In this section we prove lower bounds on the values of $N(m,k,r)$. The simplest case is when $k=2$, where we have

$$N(m,2,r) = \sum_{i=1}^{r} \binom{m}{i} . \tag{1}$$

This follows from the fact that each column can have $j$ ones, $1 \leq j \leq r$, but no column can occur more than once.
Next we will show that it suffices to consider even dependencies only.

**Proposition 2.1** *Let $A$ be a 0-1-matrix with dimension $m \times n$. Then there exists an $m \times n/2$ submatrix $A'$ of $A$, such that no odd number of columns of $A'$ is linearly dependent.*
*In particular, for integers $k, r \geq 1$,*

$$N(m,2k+1,r) \geq \frac{1}{2} \cdot N(m,2k,r) . \tag{2}$$

Let $A$ be an $m \times n$ matrix over $\{0,1\}$. Choose rows of $A$ at random, independently of each other, with probability $1/2$. Let $B$ be the resulting random set of rows. Let $c$ be a column in $A$ with exactly $f$ ones. Then the probability $Prob$ that column $c$ has an odd number of ones within the rows of $B$ is given by

$$Prob = \sum_{i=0}^{\lfloor \frac{f-1}{2} \rfloor} \binom{f}{2i+1} \cdot \left(\frac{1}{2}\right)^{f} = \frac{1}{2} .$$

Thus the expected number of columns of $A$, having an odd number of ones within the rows of $B$ is exactly $n/2$. Hence, there exists a choice of these $n/2$ columns. Call the resulting $m \times n/2$ matrix $C$. By a parity argument, each odd number of columns in $C$ is linearly independent.
Inequality e50 follows by taking a $(2k,r)$-matrix $A$ with dimension $m \times n$, where $n = N(m,2k,r)$. By monotonicity, we have $N(m,k,r) \geq N(m,k+1,r)$. This, together with Proposition 2.1 yields

**Corollary 2.2** *For integers $k, r \geq 1$,*

$$\frac{1}{2} \cdot N(m,2k,r) \leq N(m,2k+1,r) \leq N(m,2k,r) .$$

Next, we will show for arbitrary, but fixed values of $k$ and $r$ a lower bound on $N(m,k,r)$.

**Theorem 2.3** *Let $k \geq 2$ and $r \geq 1$ be fixed integers. Then, for $m$ large,*

$$N(m,k,r) = \Omega\left(m^{\frac{kr}{2(k-1)}}\right) .$$

Consider an $m \times n$ matrix whose columns are chosen independently from the uniform distribution on all columns with exactly $r$ ones. Assume that the sum of $i$ of these columns is the zero vector. Then $ir$ is even and the $ir$ ones in these columns are all contained in at most $ir/2$ rows. For a fixed $i$, the expected number $S_i$ of such situations is at most

$$\binom{n}{i} \cdot \sum_{j=r}^{ir/2} \binom{m}{j} \frac{\binom{j}{r}^i}{\binom{m}{r}^i} = O\left(n^i m^{-\frac{ir}{2}}\right) .$$

Denote by $S = \sum_{i=2}^{k} S_i$ the sum of these expectations. Let $n = \lceil \varepsilon m^{\frac{kr}{2(k-1)}} \rceil$, where $\varepsilon = \varepsilon(k,r) > 0$ is a sufficiently small constant. For $m$ large enough, we have $n \geq 2 \cdot m^{r/2}$. Thus, $S \leq c \cdot (n \cdot m^{-r/2})^k$ for some positive constant $c = c(k,r)$. Now, it is easy to verify that for $\varepsilon \leq \sqrt[k-1]{1/(2c)}$ we have $S \leq n/2$. Thus there exists an $m \times n$ matrix with no more than $n/2$ dependent groups of columns of size at most $k$. By deleting at most $n/2$ columns, for each dependent group one involved column, we obtain a $(k,r)$-matrix with $m$ rows and at least $n/2$ columns.
The arguments in the proof of Theorem 2.3 can be made constructive as follows. By using the method of conditional probabilities, cf. [AS 92], we will give a deterministic polynomial time algorithm, which yields a $(k,r)$-matrix with dimension $m \times \Omega\left(m^{\frac{kr}{2(k-1)}}\right)$, where $k \geq 2, r \geq 1$ are fixed integers. To do so, we determine first all dependent groups $F$, $|F| \leq k$, of pairwise distinct columns of length $m$ with exactly $r$ ones, where every proper subset of $F$ is independent. As the number of row-indices of the ones in each dependent group of size at most $k$ is at most $kr/2$, it is straightforward to find all such dependent groups in time $O\left(m^{kr/2}\right)$.
Let $\mathcal{F}$ denote the set of all such groups. Let $c_1, \ldots, c_t$, $t = \binom{m}{r}$, be the columns of length $m$ with exactly $r$ ones. To each column $c_i$ we associate a 'probability' $p_i$ i.e., $0 \leq p_i \leq 1$, $i = 1, \ldots, t$. Define a 'potential' $V(p_1, \ldots, p_t)$ by

$$V(p_1, \ldots, p_t) = \sum_{i=1}^{t} p_i - \sum_{F \in \mathcal{F}} \prod_{i; c_i \in F} p_i .$$

Then $V(p_1, \ldots, p_t)$ is equal to the expected difference between the number of chosen columns and the number of arising dependent groups of columns of size at most $k$, if in a random experiment each column $c_j$, $j = 1, \ldots, t$, is chosen with probability $p_j$, independently of the other choices.
For $i = 3, \ldots, k$, let $\mathcal{F}_i = \{F \in \mathcal{F} \mid |F| = i\}$. Notice that $|\mathcal{F}_i| \leq c \cdot m^{ir/2}$ for some positive constant $c = c(k,r)$.
We want to start the algorithm with a high potential, thus, in the beginning we set $p_1 = \ldots = p_t = p$, where

$$p = \varepsilon \cdot m^{\frac{2r-kr}{2(k-1)}} ,$$

and $0 < \varepsilon < (5 \cdot c \cdot r!)^{-1/(k-1)}$. (We shall still use the $p_1, \ldots, p_t$ to denote different occurrences of $p$ in the expression $V(p, \ldots, p)$!) For this choice of $\varepsilon$ and $p$, we have $V(p, \ldots, p) \geq \frac{pt}{2} = \Omega\left(m^{\frac{kr}{2(k-1)}}\right)$ for fixed $k, r \geq 2$ and $m$ sufficiently large. Namely,

$$\begin{aligned} V(p, \ldots, p) &= p \cdot t - \sum_{i=2}^{k} |\mathcal{F}_i| \cdot p^i \geq p \cdot t - \sum_{i=3}^{k} c \cdot m^{ir/2} \cdot p^i \\ &\geq p \cdot t - 2 \cdot c \cdot m^{kr/2} \cdot p^k \geq pt/2 \cdot \left(2 - 4 \cdot c \cdot t^{-1} \cdot m^{kr/2} \cdot p^{k-1}\right) \\ &\geq pt/2 \cdot \left(2 - 5 \cdot c \cdot r! \cdot m^{kr/2-r} \cdot p^{k-1}\right) \geq pt/2 \cdot \left(2 - 5 \cdot c \cdot r! \cdot \varepsilon^{k-1}\right) \geq pt/2 , \end{aligned}$$

where we used $4/t = 4/\binom{m}{r}^{-1} \leq 5 \cdot r!/m^r$ for $m$ sufficiently large.

As $V(p_1, p_2, \ldots, p_t) = (1 - p_1) \cdot V(0, p_2, \ldots, p_t) + p_1 \cdot V(1, p_2, \ldots, p_t)$, there exists $\beta_1 \in \{0, 1\}$, such that

$$V(\beta_1, p_2, \ldots, p_t) \geq V(p_1, p_2, \ldots, p_t) \ .$$

Now we replace one after the other each $p_i$ by 0 or 1 as to maximize the value of the potential. Namely, if $V(1, p_2, \ldots, p_t) > V(0, p_2, \ldots, p_t)$, then set $\beta_1 = 1$, otherwise let $\beta_1 = 0$.
If $\beta_1 = 1$, then we take column $c_1$, otherwise we discard $c_1$. This decision will not be changed later. Doing the same for $i = 2, \ldots, t$ applied to $V(\beta_1, \ldots, \beta_{i-1}, p_i, \ldots, p_t)$, we obtain a 0-1-sequence $(\beta_1, \ldots, \beta_t)$, such that for $j = 1, \ldots, t$ we have

$$V(\beta_1, \ldots, \beta_j, p_{j+1}, \ldots, p_t) \geq V(\beta_1, \ldots, \beta_{j-1}, p_j, \ldots, p_t) \ ,$$

i.e. the conditional expected difference between the number of chosen columns and the number of dependent groups of size at most $k$ does not decrease. Finally,

$$V(\beta_1, \ldots, \beta_t) \geq V(p, \ldots, p) = \Omega\left(m^{\frac{kr}{2(k-1)}}\right) \ . \tag{3}$$

Let $A$ be the matrix arising from the chosen column vectors. By eq23, $A$ is an $m \times \Omega\left(m^{\frac{kr}{2(k-1)}}\right)$ matrix. We claim that $A$ is a $(k, r)$-matrix:

**Claim 2.4** *The columns of $A$ are $k$-wise independent.*

Assume for contradiction, that the columns $c_{i_1}, \ldots, c_{i_g}$, $g \leq k$ and $i_1 < \ldots < i_g$, belong to $A$ and are dependent. In the above algorithm, the decision about each column $c_{i_j}$, $j < g$, was done before column $c_{i_g}$ was decided in step $s = i_g$.
Let $\mathcal{F}_i'$, $i = 1, \ldots, k$, be the set of all $i$-element subsets of $\{c_s, \ldots, c_t\}$, which contain $c_s$ and which yield with some of the already chosen column vectors $c_i$ (i.e. $\beta_i = 1$), $i = 1, \ldots, s-1$, an at most $k$-element set of dependent columns. As $c_{i_1}, \ldots, c_{i_g}$ are dependent, we have $|\mathcal{F}_1'| \geq 1$. We infer

$$\begin{aligned} & V(\beta_1, \ldots, \beta_{s-1}, 1, p, \ldots, p) - V(\beta_1, \ldots, \beta_{s-1}, p, \ldots, p) \\ = \ & (1-p) + \sum_{i=1}^{k} (p^i - p^{i-1}) \cdot |\mathcal{F}_i'| \\ = \ & (1-p) - (1-p) \cdot |\mathcal{F}_1'| - \sum_{i=2}^{k} (1-p) \cdot p^{i-1} \cdot |\mathcal{F}_i'| \\ \leq \ & 0 \ . \end{aligned}$$

Thus, according to our strategy, column $c_s$ would not have been chosen during the algorithm, i.e. $\beta_s = 0$, and hence, $c_{i_1}, \ldots, c_{i_g}$ are linearly independent. As each column belongs to at most $O\left(m^{(k-2)r/2}\right)$ dependent groups of size at most $k$, the running time of the algorithm is $O\left(m^{kr/2}\right)$.
□

# 3 Upper Bounds

In this section we give upper bounds on $N(m, k, r)$. Frankl and Füredi proved in [FF 86] the following result. If $H_r(m)$ denotes the largest size of a family $\mathcal{F} \subseteq [X]^r$ of $r$-element subsets of an $m$-element set such that there are no four sets $F_1, \ldots, F_4 \in \mathcal{F}$ with

$$(*) \qquad F_1 \cup F_2 = F_3 \cup F_4 \quad \text{and} \quad F_1 \cap F_2 = F_3 \cap F_4 \ ,$$

then

$$H_r(m) = \Theta\left(m^{\lceil 4r/3 \rceil / 2}\right) \ .$$

As sets $F_1, \ldots, F_4 \in [X]^r$, which satisfy $(*)$, yield a set of four dependent vectors, we obtain

**Theorem 3.1** **[FF 86]** *For fixed $r \geq 1$,*

$$N(m,4,r) = O\left(m^{\lceil 4r/3 \rceil/2}\right) .$$

Notice, that Theorem 2.3 yields $N(m,4,r) = \Omega(m^{2r/3})$.
In the following, we shall prove two recurrence relations which give upper bounds on $N(m,k,r)$, in particular, for $k$ a power of two. The first one is slightly weaker than the second one, but its proof is simpler and for many parameters it gives asymptotically the same bounds.

**Theorem 3.2** *Let $k \geq 4$, $k$ even, and let $r \geq 1$. Let $0 \leq s < r$ be arbitrary. Then*

$$N(m,k,r) \leq 2 \cdot N(m,k/2,2r-2s) + \sum_{i=1}^{s} \binom{m}{i} , \tag{4}$$

*and*

$$N(m,k,r) \leq \sqrt{2 \cdot \binom{r-1}{s} \cdot \binom{m}{s} \cdot N(m,k/2,2r-2s)} + \binom{m}{s} + \sum_{i=1}^{s} \binom{m}{i} . \tag{5}$$

*Thus for fixed $r, s, k$,*

$$N(m,k,r) = O(\sqrt{m^s \cdot N(m,k/2,2r-2s)} + m^s) . \tag{6}$$

(1) First we will show inequality e11. Let $A$ be an $m \times n$ matrix, $n = N(m,k,r)$, where $A$ is a $(k,r)$-matrix. Divide the columns of $A$ into two parts. The first part will have columns $c_1, \ldots, c_{n_1}$, $n_1$ even, such that the columns $c_{2i-1}$ and $c_{2i}$ have at least $s$ common ones, $i = 1, \ldots, n_1/2$. The second part, with $n_2$ columns, has the property that every two distinct columns have less than $s$ common ones. Clearly, such a decomposition can be constructed by choosing one after the other pairs for the first part until no such pair exists anymore. Let $B$ be the matrix with columns $c_1 \oplus c_2, c_3 \oplus c_4, \ldots, c_{n_1-1} \oplus c_{n_1}$, where $\oplus$ denotes the componentwise addition modulo 2. Observe that each two columns in $B$ are distinct, as the columns of $A$ are 4-wise independent. We infer that $B$ is a $(k/2, 2r-2s)$-matrix, thus $n_1 \leq 2 \cdot N(m,k/2,2r-2s)$. Notice, that each column in the second part with at least $s$ ones is uniquely determined by a subset of its ones of size $s$, thus $n_2 \leq \sum_{i=1}^{s} \binom{m}{i}$, and (4) follows.
(2) Next we will prove inequality e2. Let $A$ be a $(k,r)$-matrix with dimension $m \times n$, where $n = N(m,k,r)$. Divide the columns of $A$ into two parts as follows. In the first part we put each column which shares at least $s$ ones with another column of $A$, in the second part we put the rest. Let $A_1$ and $A_2$ be the arising matrices. Denote by $n_1$ and $n_2$ the number of columns in $A_1$ and $A_2$, respectively. The same argument as above gives $n_2 \leq \sum_{i=1}^{s} \binom{m}{i}$.
It remains to estimate $n_1$. For every $s$-element subset $S$ of rows, we denote by $d(S)$ the number of columns in $A_1$ which have only ones in these rows. Then,

$$N_1 := \sum_{S} d(S) = \sum_{c \in A_1} \binom{|c|}{s} , \tag{7}$$

where we sum over all columns $c$ of $A_1$ and $|c|$ denotes the number of ones in $c$. As each column in $A_1$ contains at least $s$ ones, we have

$$n_1 \leq N_1 . \tag{8}$$

The Cauchy-Schwartz inequality, together with e4, implies

$$\sum_{S} d(S)^2 \geq \frac{N_1^2}{\binom{m}{s}} ,$$

hence,

$$\sum_S \binom{d(S)}{2} = \frac{1}{2} \cdot \sum_S d(S)^2 - \frac{1}{2} \cdot \sum_S d(S) \geq \frac{N_1^2}{2 \cdot \binom{m}{s}} - \frac{N_1}{2} = \frac{N_1 \cdot \left(N_1 - \binom{m}{s}\right)}{2 \cdot \binom{m}{s}} . \tag{9}$$

Assume for the moment that $N_1 \geq \binom{m}{s}$, then (9) yields

$$\sum_S \binom{d(S)}{2} \geq \frac{\left(N_1 - \binom{m}{s}\right)^2}{2 \cdot \binom{m}{s}} . \tag{10}$$

Consider the matrix $B$ obtained from $A_1$ by taking sums of every (unordered) pair of distinct columns of $A$, which share at least $s$ ones. Note that different pairs of columns produce different columns, since in $A_1$ the columns are 4-wise independent. As above, $B$ is a $(k/2, 2r-2s)$-matrix, i.e. the number of columns of $B$ is bounded from above by $N(m, k/2, 2r-2s)$. We shall estimate the number of (unordered) pairs of columns of $A_1$ by counting pairs, which contain ones on a particular subset $S$ of rows, and we sum over all such subsets $S$ with $|S| = s$. Since two distinct columns have at most $r-1$ common ones, we count each pair at most $\binom{r-1}{s}$ times. Hence, we obtain

$$\sum_S \binom{d(S)}{2} \leq \binom{r-1}{s} \cdot N(m, k/2, 2r-2s) . \tag{11}$$

By (10) and (11) it follows that

$$\frac{\left(N_1 - \binom{m}{s}\right)^2}{2 \cdot \binom{m}{s}} \leq \binom{r-1}{s} \cdot N(m, k/2, 2r-2s) ,$$

whence, using e5,

$$n_1 \leq N_1 \leq \sqrt{2 \cdot \binom{m}{s} \cdot \binom{r-1}{s} \cdot N(m, k/2, 2r-2s)} + \binom{m}{s} . \tag{12}$$

Recall, that we obtained (12) under the assumption that $N_1 \geq \binom{m}{s}$. Thus, either $N_1 < \binom{m}{s}$, i.e. $n_1 < \binom{m}{s}$, or we have (12). Altogether, (12) holds, and, as the number of columns of $A$ equals $n = n_1 + n_2$, assertion (5) follows.
The first recurrence relation (4) gives the next inequality. Due to rounding up this does not match the lower bound always.

**Corollary 3.3** *For integers $k > 1$, $k = 2^l$,*

$$N(m, k, r) \leq (k-1) \cdot \sum_{i=1}^{\lceil kr/2(k-1) \rceil} \binom{m}{i} . \tag{13}$$

Let $k = 2^l$. We will show (13) by induction on $l \geq 1$. For $l = 1$, i.e. $k = 2$, inequality e222 follows from eq-1.
Let $l > 1$ and let $s = \lceil 2^{l-1} r/(2^l - 1) \rceil$ and $r' = 2r - 2s = 2r - 2 \cdot \lceil 2^{l-1} r/(2^l - 1) \rceil$. First we will show that

$$\left\lceil \frac{2^{l-2} r'}{2^{l-1} - 1} \right\rceil \leq \left\lceil \frac{2^{l-1} r}{2^l - 1} \right\rceil . \tag{14}$$

To do so, we can consider the left hand side without the ceiling function. After substituting $r'$ in (14) and simplifying, we get

$$2^{l-1} r \leq (2^l - 1) \cdot \left\lceil \frac{2^{l-1} r}{2^l - 1} \right\rceil ,$$

which is true, hence (14) holds. By using e11, and applying the induction assumption and (14), we obtain

$$\begin{aligned}
N(m,k,r) &\le 2\cdot N(m,k/2,2r-2s)+\sum_{i=1}^{s} mi \\
&\le 2\cdot\left(2^{l-1}-1\right)\cdot \sum_{i=1}^{\lceil 2^{l-2}r'/(2^{l-1}-1)\rceil}\binom{m}{i}+\sum_{i=1}^{\lceil 2^{l-1}r/(2^{l}-1)\rceil}\binom{m}{i} \\
&\le 2\cdot\left(2^{l-1}-1\right)\cdot \sum_{i=1}^{\lceil 2^{l-1}r/(2^{l}-1)\rceil}\binom{m}{i}+\sum_{i=1}^{\lceil 2^{l-1}r/(2^{l}-1)\rceil}\binom{m}{i} \\
&\le \left(2^{l}-1\right)\cdot \sum_{i=1}^{\lceil 2^{l-1}r/(2^{l}-1)\rceil}\binom{m}{i}\ ,
\end{aligned}$$

which proves e222.
The second recurrence relation e2 gives in some cases better asymptotic results than the first one e11:

**Corollary 3.4** *For fixed $l,r>0$ and $k=2^l$,*

$$N(m,k,r)=O\left(m^{\lceil kr/(k-1)\rceil/2}\right)\ . \tag{15}$$

We use induction on $l$. For $l=1$, i.e. 2-independence, we have by eq-1 that $N(m,2,r)=\Theta\left(m^{\lceil\frac{2r}{1}\rceil/2}\right)=\Theta\left(m^r\right)$. Assume that (15) holds for $k=2^{l-1}$. For the induction step, $k=2^l$, set

$$s=\left\lfloor\frac{\left\lceil\frac{kr}{k-1}\right\rceil}{2}\right\rfloor\ .$$

As $s\le\lceil\frac{kr}{k-1}\rceil/2$, it suffices by (6) to prove

$$\frac{1}{2}\cdot\left(s+\frac{1}{2}\cdot\left\lceil\frac{k/2\cdot(2r-2s)}{k/2-1}\right\rceil\right)\le\frac{\left\lceil\frac{kr}{k-1}\right\rceil}{2}\ . \tag{16}$$

To see this, we show first

$$\left\lceil\frac{kr}{k-1}\right\rceil-2s\le(k-1)\cdot\left\lceil\frac{kr}{k-1}\right\rceil-kr\ . \tag{17}$$

The RHS of e42 is at least 0 and at most 1. Thus, if $\left\lceil\frac{kr}{k-1}\right\rceil$ is even, then inequality (17) holds. If $\left\lceil\frac{kr}{k-1}\right\rceil$ is odd, then, as $k$ is even, the RHS of e42 is odd, i.e. is at least 1, and (17) follows.
Now inequality (17) is equivalent to

$$\frac{k\cdot(r-s)}{k/2-1}\le 2\cdot\left(\left\lceil\frac{kr}{k-1}\right\rceil-s\right)\ .$$

As its RHS is an integer, we have

$$\left\lceil\frac{k\cdot(r-s)}{k/2-1}\right\rceil\le 2\cdot\left(\left\lceil\frac{kr}{k-1}\right\rceil-s\right)\ ,$$

which yields (16), and hence (15) is proved.
This is still not the best bound which can be derived from the recurrence relation (5). In some cases we can get better bounds. For instance, for $k = 2^l$ fixed, we obtain, cf. Section 4,

$$N(m,k,2) = O\left(m^{1+2/k}\right) .$$

However, such an upper bound (with a slightly worse constant) was proved by Bondy and Simonovits [BS 74] for all even $k$. We list the best bounds which can be obtained from (5) for some small values of $k$ and $r$ in the appendix.

## 4 Graphs – The Case r=2

Here we consider the special case $r = 2$. Then, $N(m,k,2)$ denotes the maximum number of one-element and two-element edges in a graph on $m$ vertices, such that no $j$ edges, $j = 1, 2, \ldots, k$, form a subgraph where each vertex is covered an even number of times. By Theorem 2.3 we have $N(m,k,2) = \omega(m)$ for every fixed $k > 1$. Thus, asymptotically we may neglect the one-element sets, and therefore the growth rate of $N(m,k,2)$ is equal to the maximum number of (two-element) edges in a graph on $m$ vertices, not containing any cycle $C_3, C_4, \ldots, C_k$. Concerning the growth rate of $N(m,k,2)$, it suffices to consider only cycles of even length, cf. Proposition 2.1.
For a family $\mathcal{G}$ of forbidden subgraphs, let $ex(m,\mathcal{G})$ denote the maximum number of edges in a graph on $m$ vertices without containing any copy of a forbidden subgraph $G \in \mathcal{G}$.
Clearly, $N(m,2,2), N(m,3,2) = \Theta(m^2)$. Extending earlier work of Erdős [Er 38], Erdős, Renyi and Sós [ERS 66] and Brown [Br 66] proved:

$$ex(m,C_4) = \frac{1}{2} \cdot m^{3/2} + O(m^{4/3}) , \tag{18}$$

thus,

$$N(m,4,2) \leq (1/2 + o(1)) \cdot m^{3/2} .$$

We give a simple construction which yields $N(m,4,2) \geq (1/(2\sqrt{2}) - o(1)) \cdot m^{3/2}$. Namely, let $q$ be the largest prime power with $q^2 \leq m$. Define a bipartite graph $G = (V_1 \cup V_2, E)$ with vertex set $V_1 = V_2 = (GF(q))^2 \setminus \{(0,0)\}$ and edges $\{\underline{p}, \underline{q}\} \in E$ with $\underline{p} \in V_1$ and $\underline{q} \in V_2$, if and only if $\underline{p} \cdot \underline{q} = 1$, where '$\cdot$' denotes the usual componentwise scalar product.
Assume that $G$ contains a 4-cycle $C_4$ given by the edges $\{\underline{p_1}, \underline{p_2}\}, \{\underline{p_2}, \underline{p_3}\}, \{\underline{p_3}, \underline{p_4}\}, \{\underline{p_1}, \underline{p_4}\}$, say, $\underline{p_1}, \underline{p_3} \in V_1$ and $\underline{p_2}, \underline{p_4} \in V_2$. Then, $\underline{p_1} \cdot \underline{p_2} = \underline{p_2} \cdot \underline{p_3} = \underline{p_3} \cdot \underline{p_4} = \underline{p_1} \cdot \underline{p_4} = 1$. Thus, $\underline{p_1} \cdot (\underline{p_2} - \underline{p_4}) = \underline{0}$ and $\underline{p_3} \cdot (\underline{p_2} - \underline{p_4}) = \underline{0}$. As $\underline{p_2} \neq \underline{p_4}$, the vectors $\underline{p_1}$ and $\underline{p_3}$ are collinear, i.e. $\underline{p_1} = \lambda \cdot \underline{p_3}$ for some $\lambda \in GF(q)$. With $\underline{p_1} \cdot \underline{p_2} = 1$ and $\underline{p_2} \cdot \underline{p_3} = 1$ we infer $\lambda = 1$, i.e. $\underline{p_1} = \underline{p_3}$, but $\underline{p_1}, \underline{p_3} \in V_1$, which is a contradiction. A simple counting argument gives $|E| = (1 - o(1)) \cdot q^3$. The graph $G$ is bipartite, hence triangle-free, and has $2 \cdot (p^2 - 1)$ vertices. This implies $N(m,4,2) \geq (1/(2\sqrt{2}) - o(1)) \cdot m^{3/2}$. Thus, we have shown

**Proposition 4.1**

$$\left(\frac{1}{2\sqrt{2}} - o(1)\right) \cdot m^{3/2} \leq N(m,4,2) \leq \left(\frac{1}{2} + o(1)\right) \cdot m^{3/2}. \tag{19}$$

□

Indeed, as mentioned in [Fű 91], Erdős and Simonovits conjecture that

$$ex(m, \{C_3, C_4\}) = \frac{1 + o(1)}{2\sqrt{2}} \cdot m^{3/2} .$$

By a probabilistic argument, Erdős showed [Er 59] that $ex(m,\{C_3,\ldots,C_{2k}\}) \geq c\cdot m^{1+\frac{1}{2k}}$ for some positive constant $c = c(k)$. Notice, that the probabilistic argument with deletion, cf. the proof of Theorem 2.3, yields $ex(m,\{C_3,\ldots,C_{2k}\}) \geq c\cdot m^{1+\frac{1}{2k-1}}$.
By a result of Bondy and Simonovits [BS 74], every graph on $m$ vertices with at least $90km^{(k+1)/k}$ edges contains cycles of length $2l$ for $l = k,\ldots,km^{1/k}$, hence,

$$c_1\cdot m^{1+\frac{1}{2k-1}} \leq N(m,2k,2) \leq 90\cdot k\cdot n^{1+\frac{1}{k}} \tag{20}$$

for every fixed positive integer $k$.
The following gives a slight improvement on the constant factor in the upper bound in eq26.

**Proposition 4.2** *For fixed integers $k\geq 4$, $k = 2^l$,*

$$N(m,k,2) \leq (1+o(1))\cdot 2^{\frac{k-8}{k}}\cdot m^{1+\frac{2}{k}} \leq (2+o(1))\cdot m^{1+\frac{2}{k}}\ .$$

For $k = 4$, we have $N(m,4,2) \leq (1/2+o(1))\cdot m^{3/2}$ by eq19a. Moreover, by e2 we obtain for $s = 1$,

$$N(m,k,2) \leq \sqrt{2\cdot m\cdot N(m,k/2,2)} + 2m\ . \tag{21}$$

If we assume that $N(m,k/2,2) \leq (1+o(1))\cdot 2^{\frac{k-16}{k}}\cdot m^{1+\frac{4}{k}}$, then, using eq20a, we infer in the induction step that

$$\begin{aligned} N(m,k,2) &\leq \sqrt{2^{\frac{2k-16}{k}}\cdot(1+o(1))\cdot m^{2+\frac{4}{k}}} + 2m \\ &\leq (1+o(1))\cdot 2^{\frac{k-8}{k}}\cdot m^{1+\frac{2}{k}}, \end{aligned}$$

as desired.
Constructions of graphs on $m$ vertices with $\Omega(m^{(k+1)/k})$ edges, which have no cycles of lengths $3,\ldots,2k$, are known only for $k = 2,3,5$. In particular, Benson [Be 66] gave an algebraic construction, while Wenger [We 90] used finite projective geometries.
Using the so called Ramanujan Graphs, Lubotzky, Phillips and Sarnak [LPS 88] and Margulis [Ma 88] have improved the probabilistic lower bound to $ex(m,\{C_3,\ldots,C_{2k}\}) = \Omega(m^{\frac{3k+5}{3k+3}})$, hence,

$$N(m,2k,2) \geq c\cdot n^{\frac{3k+5}{3k+3}} = c\cdot n^{1+\frac{2}{3k+3}}\ .$$

Recent constructive improvements by Lazebnik, Ustimenko and Woldar [LUW 95] on the lower bound on $ex(m;\{C_3,\ldots,C_{2k}\})$ imply

$$N(m,2k,2) = \Omega\left(m^{1+\frac{2}{3k-3+\varepsilon}}\right)\ ,$$

where $\varepsilon\in\{0,1\}$, and $\varepsilon = 0$ if and only if $k$ is an odd integer.

# 5 Explicit Constructions

**Construction 1.** First we will give a construction, which yields $N(m,4,3) \geq (1/8-o(1))\cdot m^2$. We use the notion of 3-uniform hypergraphs. Let $X$ be an $m$-element set. Any three triples cannot cover a set, where each vertex contains an even number of triples. Now, 4-wise independence of triples means, that the corresponding 3-uniform hypergraph $\mathcal{G} = (X,\mathcal{F})$, $\mathcal{F}\subseteq[X]^3$, does not contain any subhypergraph isomorphic to one of three configurations $V_1, V_2, V_3$. Namely, for distinct vertices $x_1,\ldots,x_6$, these are:

$$\begin{aligned} V_1 &= \{\{x_1,x_2,x_3\},\{x_1,x_3,x_4\},\{x_2,x_5,x_6\},\{x_4,x_5,x_6\}\} \\ V_2 &= \{\{x_1,x_2,x_3\},\{x_1,x_3,x_4\},\{x_1,x_4,x_5\},\{x_1,x_2,x_5\}\} \\ V_3 &= \{\{x_1,x_2,x_3\},\{x_1,x_4,x_5\},\{x_2,x_4,x_6\},\{x_3,x_5,x_6\}\}\ . \end{aligned}$$

To see that these are the only configurations, recall that each vertex in such a configuration must be covered either four times or twice. The only possibilities to distribute 12 in such a way are $(4,4,4)$, $(4,4,2,2)$, $(4,2,2,2,2)$ and $(2,2,2,2,2,2)$. The first two cannot be realized, and the third determines uniquely $V_2$. The last possibility gives $V_1$ and $V_2$; these two are uniquely determined by the condition of having, respectively not having, two vertices contained in two edges.
Observe, that in Steiner triple systems (each two-element subset is covered exactly once) the configurations $V_1$ or $V_2$ do not occur. However, for $m \equiv 1$ or $3 \mod 6$, Steiner triple systems on $m$ points exist and have $1/3 \cdot m2$ triples. Having this in mind, we consider a triple system with vertex set $X = Z_n \times \{0,1\}$, where $n$ is odd. The family $\mathcal{F}$ consists of all triples $\{(x,0),(y,0),(x+y,1)\}$ with $x, y \in Z_n$, $x \neq y$, and additions are done modulo $n$. Clearly, $|\mathcal{F}| = n2$, and distinct triples share at most one vertex. Thus, it suffices to show that $V_3$ does not occur in $(X, \mathcal{F})$. Suppose it does. By symmetry, we can assume that $x_i = (y_i, 0)$, $i = 1,2$, and $x_3 = (y_1 + y_2, 1)$. Observe, that in each triple of the system there is exactly one vertex with the second coordinate equal to 1. Then considering $\{x_3, x_5, x_6\}$, we infer $x_5 = (y_5, 0)$, hence, $x_4 = (y_1 + y_5, 1)$. We obtain $x_6 = (y_1 + y_2 - y_5, 0)$ using $\{x_3, x_5, x_6\}$, and $x_6 = (y_1 + y_5 - y_2, 0)$ using $\{x_2, x_4, x_6\}$, whence $2 \cdot (y_2 - y_5) \equiv 0 \mod n$. As $n$ is odd, this implies $y_2 \equiv y_5 \mod n$, i.e. $y_2$ and $y_5$ are not distinct, and therefore, $V_3$ does not occur in $(X, \mathcal{F})$. Thus we have shown the following

**Proposition 5.1** *There is an explicit construction of $(4,3)$-matrices with dimension $m \times n$ such that*

$$n = (1/8 - o(1)) \cdot m^2.$$

□

In the following, we will describe some general constructions of $(k,r)$-matrices for fixed integers $k, r$.

**Construction 2.** The next construction gives $N(m,k,r) = \Omega(m^{2r/k})$.

**Proposition 5.2** *Let $M$ be an $s \times n$ matrix with $k$-wise independent columns. Then, for every integer $r > 1$, one can construct a $(k,r)$-matrix $M'$ with dimension $m \times n$ such that $m \leq r \cdot 2^{\lceil s/r \rceil}$.*

Divide $M$ into $r$ matrices with dimensions $\lceil s/r \rceil \times n$ and $\lfloor s/r \rfloor \times n$. In each of the matrices encode the nonzero columns by columns of dimension $2^{\lceil s/r \rceil}$, respectively $2^{\lfloor s/r \rfloor}$, which have exactly one 1 and encode the zero columns by zero columns of the corresponding larger dimension. By putting the expanded matrices together we get the matrix $M'$.

**Corollary 5.3** *There is an explicit construction of $(k,r)$-matrices with dimension $m \times n$ such that $n = \Omega(m^{2r/k})$.*

Take the parity check matrix $M$ for a BCH code with odd distance $k+1$ and length $n$, where $n+1$ is a power of 2. Then, in terms of Proposition 5.2, we have $s = k/2 \cdot \log(n+1)$, which gives a $(k,r)$-matrix with dimension $m \times n$, where

$$m \leq r \cdot 2^{\left\lceil \frac{k \log(n+1)}{2r} \right\rceil} \leq r \cdot 2^{\frac{k \log(n+1)}{2r} + 1} = 2r \cdot (n+1)^{\frac{k}{2r}}.$$

Since the set of powers of 2 is sufficiently dense, we obtain asymptotically the bound $n = \Omega(m^{2r/k})$ for all $m$.

**Construction 3.** The above construction is the best that we know of for $r$ large with respect to $k$. If $k \geq 2r$ it is useless. We give another one, which is better for $k \gg r$. It is based on the following recursive construction, which in a sense is reverse to the one given above.
Let $M_1, \ldots, M_s$ be matrices such that $M_i$ is a $(k, r_i)$-matrix with dimension $m_i \times n_i$, $i = 1, \ldots, s$. Let $M$ be an $n \times m$ matrix with $k$-wise independent columns and exactly $s$ ones in each column.

Furthermore, we assume that we can divide the rows of $M$ into $s$ blocks $B_1, \ldots, B_s$ so that each column contains exactly one 1 in each of the blocks and $|B_i| = m_i$. We can identify rows in each block $B_i$ with the columns of $M_i$. Then each column in $M$ determines one column in each of the matrices $M_1, \ldots, M_s$. We construct a new matrix $M'$ by replacing each column of $M$ by the concatenation of the corresponding columns in $M_1, \ldots, M_s$.

**Claim 5.4** *The columns in $M'$ are $k$-wise independent.*

Suppose that $k$ columns in $M'$ are dependent. Consider the parts of these columns which come from matrix $M_i$ for some $i$. Since each $k$ columns of $M_i$ are independent, each of these parts must occur an even number of times. If we consider the corresponding $k$ columns in $M$, then the above property implies that in each row we have an even number of ones, a contradiction.
Let us observe that the condition that the rows of $M$ can be split into blocks such that each column contains exactly one 1 is not an essential restriction. If $M$ does not satisfy this condition, we can replace it by a matrix with the same number of columns and with $sn$ ones, where we put the first 1 of each column in the block $\{1, \ldots, n\}$, the second one in the block $\{n+1, \ldots, 2n\}$, and so on. As there exists a linear transformation which maps the columns of the new matrix on the old one, each $k$ columns of the new one must be independent, hence

**Proposition 5.5** *Let $k, r, s \geq 2$ be fixed. Suppose that there are constructions of (1) $(k, r)$-matrices with $n$ rows and $\Omega(n^t)$ columns and (2) $(k, s)$-matrices with $n$ rows and $\Omega(n^u)$ columns. Then there is a construction of $(k, r \cdot s)$-matrices with $n$ rows and $\Omega(n^{tu})$ columns.*

Taking, for $r = 2$, the known constructions for $k = 4, 6$ and 10 and the general construction of Lubotzky, Phillips and Sarnak, cf. Section 4, we get:

**Corollary 5.6**
*(1) Let $k \in \{4, 6, 10\}$ and let $r$ be a power of 2. Then there exists a construction of $(k, r)$-matrices with $m$ rows and*

$$\Omega\left(m^{(1+2/k)^{\log r}}\right)$$

*columns.*
*(2) Let $k$ be even and let $r$ be a power of 2. Then there exists a construction of $(k, r)$-matrices with $m$ rows and*

$$\Omega\left(m^{\left(1+\frac{4}{3k+3}\right)^{\log r}}\right)$$

*columns.*

For example, we get a construction of $(4, 4)$-matrices with $m$ rows and $\Omega(m^{2.25})$ columns.

**Construction 4.** We shall present one more construction, which gives

$$N(m, 4, r) = \Omega\left(m^{\lceil r/2 \rceil}\right).$$

Instead of 0-1-matrices $M$, where each four columns are independent and each column contains exactly $r$ ones, we consider families of $r$-element subsets of an $m$-element set $X$ without the corresponding prohibited configurations, which are the configurations of linearly dependent sets. The sets $F_1, \ldots, F_k$ are called dependent if the associated 0,1-columns are linearly dependent, otherwise they are called independent. Let $\mathcal{F} \subseteq [X]^r$ be the family arising from such a matrix $M$. By Proposition 2.1, we may assume that there are no three dependent sets. First we need some preliminary considerations. Let $F_1', F_2', F_3', F_4' \in \mathcal{F}$ be distinct dependent sets. Let $S = \bigcap_{i=1}^4 F_i'$, $|S| = s$, and set $F_i = F_i' \setminus S$, $i = 1, \ldots, 4$. By subtracting $|F_1 \cap F_2|$ from both sides of $|F_1| = |F_2|$, we obtain $|F_1 \cap F_3| + |F_1 \cap F_4| = |F_2 \cap F_3| + |F_2 \cap F_4|$. Similarly, from $|F_3| = |F_4|$, we infer $|F_1 \cap F_3| + |F_2 \cap F_3| = |F_1 \cap F_4| + |F_2 \cap F_4|$. Hence,

$$|F_1 \cap F_3| = |F_2 \cap F_4| \ . \tag{22}$$

Analogously, one may obtain

$$|F_1 \cap F_2| = |F_3 \cap F_4|$$

and

$$|F_1 \cap F_4| = |F_2 \cap F_3| \ .$$

The set $F_1$ is a disjoint union of $F_1 \cap F_2$, $F_1 \cap F_3$ and $F_1 \cap F_4$. If two of these intersections are empty, $F_1$ would be a subset of one of the sets $F_2$, $F_3$ or $F_4$. This is not true, hence at most one of the intersections $F_1 \cap F_2$, $F_1 \cap F_3$ and $F_1 \cap F_4$ is empty. If one of them is empty, we say that the configuration is of type $\mathcal{V}_1^{(r)}$. In this case, we infer with eq31q and the following identities, that there are two pairs of distinct sets $F_i, F_j$ with empty intersection. If all the intersections are nonempty, we say that the configuration is of type $\mathcal{V}_2^{(r)}$.
Note, that in each configuration from $\mathcal{V}_1^{(r)}$ or $\mathcal{V}_2^{(r)}$, there is at least one intersection $F_i \cap F_j$ satisfying $0 < |F_i \cap F_j| \leq \lfloor r/2 \rfloor$. Moreover, in configurations of type $\mathcal{V}_2^{(r)}$, there is an intersection satisfying $0 < |F_i \cap F_j| \leq \lfloor r/3 \rfloor$.
Next we will describe a family $\mathcal{F}_r(c_1, \ldots, c_{\lfloor r/2 \rfloor}) \subseteq [X]^r$ of sets, depending on parameters $c_1, \ldots, c_{\lfloor r/2 \rfloor} \in X$, where $X = Z_p$, $p$ a prime and $p > \lfloor r/2 \rfloor$. We shall prove that for appropriate values of these parameters, the family does not contain any four dependent sets. Let $F \in \mathcal{F}_r(c_1, \ldots, c_{\lfloor r/2 \rfloor})$ if and only if

$$\sum_{f \in F} f^j = c_j \qquad \text{for } j = 1, \ldots, \lfloor r/2 \rfloor. \tag{23}$$

For the proof, we will need the following lemma.

**Lemma 5.7** *Let $F_1', \ldots, F_4' \in [Z_p]^r$ be dependent sets. Let $S = \bigcap_{i=1}^4 F_i'$, $|S| = s$, and set $F_i = F_i' \backslash S$, $i = 1, \ldots, 4$. Denote the intersections $|F_i \cap F_j|$ as $A, B, \ldots, F$, so that $F_1 = A \cup B \cup C$, $F_2 = A \cup D \cup E$, $F_3 = B \cup D \cup F$, and $F_4 = C \cup E \cup F$. If there exists a constant $c$ such that*

$$\sum_{f \in F_i'} f^j = c$$

*for $i = 1, 2, 3, 4$ and some $j$, then*

$$\sum_{f \in B} f^j = \sum_{f \in E} f^j, \ \ \sum_{f \in A} f^j = \sum_{f \in F} f^j, \ \ \sum_{f \in C} f^j = \sum_{f \in D} f^j \ . \tag{24}$$

We have

$$\sum_{f \in A \cup B \cup C} f^j = c \tag{25}$$

$$\sum_{f \in A \cup D \cup E} f^j = c \tag{26}$$

$$\sum_{f \in B \cup D \cup F} f^j = c \tag{27}$$

$$\sum_{f\in C\cup E\cup F} f^j = c. \tag{28}$$

Subtracting lk101 and lk102 as well as lk103 and lk104, we obtain

$$\sum_{f\in B\cup C} f^j = \sum_{f\in D\cup E} f^j \tag{29}$$

$$\sum_{f\in B\cup D} f^j = \sum_{f\in C\cup E} f^j. \tag{30}$$

Equations lk105 and lk106 imply

$$\sum_{f\in B} f^j = \sum_{f\in E} f^j.$$

Similarly, the other identities in plk1 follow.
Now, assume that $F_1', \ldots, F_4' \in \mathcal{F}_r(c_1, \ldots, c_{\lfloor r/2 \rfloor})$ are dependent. Using the notation from the proof of Lemma 5.7 and by a similar argument, we infer $|B| = |E|$, $|C| = |D|$ and $|A| = |F|$. Since the sets $A, B, \ldots, F$ are pairwise disjoint and at least two of the pairs consist of nonempty sets, one of the pairs consists of nonempty sets of size at most $\lfloor r/2 \rfloor$. Wlog, assume that this is the pair $B, E$. By Lemma 5.7 and by definition of the system $\mathcal{F}_r(c_1, \ldots, c_{\lfloor r/2 \rfloor})$, we have

$$\sum_{f\in B} f^j = \sum_{f\in E} f^j$$

for all $j = 1, \ldots, \lfloor r/2 \rfloor$. To get a contradiction, we use

**Lemma 5.8** *Let $x_1, \ldots, x_s, y_1, \ldots, y_s$ be elements of some fixed field $F$, where $char(F) > s$. Suppose that*

$$\sum_{i=1}^{s} x_i^j = \sum_{i=1}^{s} y_i^j,$$

*for $j = 1, \ldots, s$. Then $\{x_1, \ldots, x_s\} = \{y_1, \ldots, y_s\}$ (in fact $(y_1, \ldots, y_s)$ is just a permutation of $(x_1, \ldots, x_s)$).*

By a well-known theorem about symmetric polynomials, the elementary symmetric polynomials

$$e_j(x_1, \ldots, x_s) = \sum_{1\le i_1 < \ldots < i_j \le s} x_{i_1} \cdot \ldots \cdot x_{i_j}$$

can be expressed as a polynomial in the symmetric polynomials $s_j(x_1, \ldots, x_s) = \sum_{i=1}^{s} x_i^j$ for $j = 1, \ldots, s$, namely, by Warings formula, cf. [Ai 75], p. 259:

$$e_j(x_1, \ldots, x_s) = \sum \frac{(-1)^{s - \sum_{i=1}^{s} b_i}}{\prod_{i=1}^{j} (b_i!) \cdot \prod_{i=1}^{j} i^{b_i}} \cdot \prod_{i=1}^{j} s_i^{b_i}(x_1, \ldots, x_s)\,, \tag{31}$$

where the summation extends over all sequences $(b_1, \ldots, b_j)$ with $\sum_{i=1}^{j} i \cdot b_i = j$. Thus the assumption of the lemma implies

$$\sum_{1\le i_1 < \ldots < i_j \le s} x_{i_1} \cdot \ldots \cdot x_{i_j} = \sum_{1\le i_1 < \ldots < i_j \le s} y_{i_1} \cdot \ldots \cdot y_{i_j} =: a_{s-j}$$

for $j = 1, \ldots, s$. Therefore, both, $-x_1, \ldots, -x_s$ and $-y_1, \ldots, -y_s$, are the roots of the polynomial $\prod_{i=1}^{s}(z + x_i) = z^s + a_{s-1}z^{s-1} + \ldots + a_0$, whence the conclusion follows.
Now we can finish our argument. By our assumption $p > \lfloor r/2 \rfloor$, and as $|B| = |E| \leq \lfloor r/2 \rfloor$, we infer with Lemma 5.8 that $B = E$, which is a contradiction.
It remains to estimate the size of the family $\mathcal{F}$. To this end, we choose suitably the constants $c_1, \ldots, c_{\lfloor r/2 \rfloor}$. Namely, the average number of solutions of the system of equations (23) is clearly $p^r / p^{\lfloor r/2 \rfloor} = p^{\lceil r/2 \rceil}$. Hence, there is a choice of the constants such that the number of solutions is at least this number. Thus, we can finish Construction 4 with

**Lemma 5.9** *There exist constants $c_1, \ldots, c_{\lfloor r/2 \rfloor}$ such that the family $\mathcal{F}_r(c_1, \ldots, c_{\lfloor r/2 \rfloor})$ determines a $(4, r)$-matrix with $m$ rows and $\Omega(m^{\lceil r/2 \rceil})$ columns.*

This implies the semiconstructive lower bound $N(m, 4, r) = \Omega\left(m^{\lceil r/2 \rceil}\right)$. Note that, for $s = \lceil (2r - 1)/3 \rceil$, it follows from e2 that $N(m, 4, r) \leq c_2 \cdot m^{\lceil 4r/3 \rceil / 2}$. The reason why the construction is not quite constructive is that the choice of the constants $c_j$ is not explicit. However, we conjecture that actually any choice of the constants gives asymptotically the same bound.

# 6 Related Extremal Problems for Hypergraphs

In contrast to the considerations in Section 5 on the growth rate of $N(m, 4, 3)$ the following should be noted. For a family $\mathcal{V}$ of forbidden configurations of triples, let $ex(m; \mathcal{V})$ denote the largest size of a family of triples on an $m$-element set, which does not contain any configuration $V \in \mathcal{V}$. In [LPR 93] it has been shown that

**Theorem 6.1 [LPR 93]** *For positive integers $m$,*

$$\begin{aligned} c_1 \cdot m^2 &\leq ex(m; V_1) \leq c_2 \cdot m^{2.5} \\ c_3 \cdot m^{2.5} &\leq ex(m; V_3) \leq c_4 \cdot m^{2.75} . \end{aligned}$$

We refer to Section 5 for the definition of $V_1, V_2, V_3$. In complementing this result, we will show here that

**Proposition 6.2**

$$ex(m; V_2) = \Theta(m^{2.5}) .$$

For the lower bound we will use an argument of [SEB 73]. For a prime power $q$ and $m = q^2 + q + 1$, there exists a Singer set $S \subseteq Z_m$, [Sin 38], i.e. each nonzero element $x \in Z_m$ can be written uniquely as $x = s_1 - s_2$ with $s_1, s_2 \in S$. Thus, $m - 1 = |S| \cdot (|S| - 1)$. Let $X$ consist of three pairwise disjoint copies $X_1, X_2, X_3$ of $Z_m$. Let $\mathcal{F} \subseteq [X]^3$ be defined by $\{f_1, f_2, f_3\} \in \mathcal{F}$ if and only if $f_i \in S_i$, $i = 1, 2, 3$, and $f_1 + f_2 + f_3 \in S$. Suppose that $(X, \mathcal{F})$ contains configuration $V_2$. Let wlog. $x_1 \in S_1$, and $x_2, x_4 \in S_2$, and $x_3, x_5 \in S_3$, and let $\mathcal{F}$ contain the triples $\{x_1, x_2, x_3\}, \{x_1, x_3, x_4\}, \{x_1, x_4, x_5\}, \{x_1, x_2, x_5\}$. Then,

$$\begin{aligned} & (x_1 + x_2 + x_3) - (x_1 + x_2 + x_5) \\ = & (x_1 + x_4 + x_3) - (x_1 + x_4 + x_5) \\ = & x_3 - x_5 . \end{aligned}$$

However, $x_2 \neq x_4$ implies $x_1 + x_2 + x_3 \neq x_1 + x_4 + x_3$, and similarly, $x_1 + x_2 + x_5 \neq x_1 + x_4 + x_5$. Thus $x_3 - x_5$ is representable in two distinct ways as a difference of two elements of $S$, which is a contradiction to our assumption that $S$ is a Singer set. As $|S| \geq (1 - o(1)) \cdot \sqrt{m}$, we have $|\mathcal{F}| \geq m^2 \cdot |S| \geq (1 - o(1)) \cdot m^{2.5}$, i.e. $ex(m; V_2) \geq 1/\sqrt{243} \cdot m^{2.5}$.

Concerning the upper bound on $ex(m; V_2)$, let $\mathcal{F}$ be a triple system on an $m$-element set $X$, where $\mathcal{F}$ does not contain configuration $V_2$. For each vertex $x \in X$, let $\mathcal{F}_{[x]} = \{F \setminus \{x\} \mid x \in F \in \mathcal{F}\}$. Then $\mathcal{F}_{[x]}$ can be seen as a graph on less than $m$ vertices. If $\mathcal{F}_{[x]}$ contains a cycle $C_4$, then $\{F \in \mathcal{F} \mid x \in F\}$ contains configuration $V_2$. By our assumption and by e200, we have $|\mathcal{F}_{[x]}| \leq (1/2 - o(1)) \cdot m^{1.5}$ for each $x \in X$, hence,

$$|\mathcal{F}| \leq \frac{\sum_{x \in X} |\mathcal{F}_{[x]}|}{3} \leq \left(\frac{1}{6} - o(1)\right) \cdot m^{2.5} .$$

This shows $ex(m; V_2) = \Theta(m^{2.5})$.
By setting $s = 2$ in the proof of Theorem 3.2, part (2) it follows that $ex(m; \{V_1, V_2\}) \leq c \cdot m^2$. Summarizing, we have $ex(m; \{V_1, V_2, V_3\}) = \Theta(m^2)$, but $ex(m; V_2), ex(m; V_3) \geq c \cdot m^{2.5}$. As $ex(m; \{V_1, V_2\}) \leq c_1 \cdot m^2$, it might be interesting to determine the growth rate of $ex(m; V_1)$.

Now, we shall investigate constructions avoiding configurations of type $\mathcal{V}_2^{(r)}$, cf. Section 5 for the definition. The construction is a variant of Construction 4. Define a family $\mathcal{F}'(c_1, \ldots, c_{\lfloor r/3 \rfloor}) \subseteq [Z_p]^r$, $p$ a prime, by $F \in \mathcal{F}'(c_1, \ldots, c_{\lfloor r/3 \rfloor})$ if and only if

$$\sum_{f \in F} f^j = c_j \qquad \text{for } j = 1, \ldots, \lfloor r/3 \rfloor$$

for suitable constants $c_j \in Z_p$. By an averaging argument, the constants $c_j$ are chosen in such a way that $|\mathcal{F}(c_1, \ldots, c_{\lfloor r/3 \rfloor})| = \Theta(m^{r - \lfloor r/3 \rfloor})$.
We claim that $\mathcal{F}(c_1, \ldots, c_{\lfloor r/3 \rfloor})$ does not contain any configuration from $\mathcal{V}_2^{(r)}$. To see this, assume that $F_1, \ldots, F_4 \in \mathcal{F}$ yield a configuration from $\mathcal{V}_2^{(r)}$. Let $A, B, \ldots, F$ be defined as in Lemma 5.7. Because of the type of our configuration, all these sets are nonempty. Hence, there is a pair of sets, say $B, E$, such that $|B| = |E| \leq \lfloor r/3 \rfloor$. Then Lemma 5.7 implies

$$\sum_{f \in B} f^j = \sum_{f \in E} f^j \qquad \text{for } j = 1, \ldots, \lfloor r/3 \rfloor .$$

Using Lemma 5.8 we infer $B = E$, which is a contradiction.
Hence, we obtain

**Lemma 6.3** *For every $r$ and $m$ large enough, there exist constants $c_1, \ldots, c_{\lfloor r/3 \rfloor}$, such that $\mathcal{F}'(c_1, \ldots, c_{\lfloor r/3 \rfloor})$ avoids configurations of type $\mathcal{V}_2^{(r)}$ and has size at least $\Omega(m^{r - \lfloor r/3 \rfloor})$.*

Thus $ex(m; \mathcal{V}^{(r)}) \geq c \cdot m^{r - \lfloor r/3 \rfloor}$. Note, that $r - \lfloor r/3 \rfloor > \lceil 4r/3 \rceil / 2$ for $r \equiv 2 \bmod 3$. However, we do not have any nontrivial upper bound on $ex(m; \mathcal{V}_2^{(r)})$.

Concerning the case $r = 4$, we give a related construction, where no configuration from $\mathcal{V}_2^{(4)}$ occurs. Let $q = 5^t$, where $t \geq 2$. Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a 4-uniform 4-partite hypergraph with $\mathcal{V} = Z_q$ and $\mathcal{E} \subseteq [\mathcal{V}]^4$. Moreover, let $\{x_1, x_2, x_3, x_4\} \in \mathcal{E}$ if and only if

$$\sum_{1 \leq i < j \leq 4} x_i x_j \equiv 1 \bmod q \qquad \text{and} \qquad x_1 \equiv \ldots \equiv x_4 \equiv 1 \bmod 5 .$$

Now $\sum_{1 \leq i < j \leq 4} x_i x_j \equiv 1 \bmod 5^t$, and, say, $x_1 \equiv x_2 \equiv x_3 \equiv 1 \bmod 5$, imply $x_4 \equiv 1 \bmod 5$. It follows that $|\mathcal{E}| = \Theta(q^3)$.
We claim that $\mathcal{G}$ does not contain any copy of the following configuration from $\mathcal{V}_2^{(4)}$:

$$\begin{aligned} A &= \{x_1, x_2, x_3, x_4\} \\ B &= \{x_3, x_5, x_7, x_8\} \\ C &= \{x_1, x_2, x_5, x_6\} \\ D &= \{x_4, x_6, x_7, x_8\} , \end{aligned}$$

where $A, B, C, D$ are pairwise distinct sets.
Suppose for contradiction, that $\mathcal{G}$ contains this configuration. We show first that $|E \cap E'| \leq 2$ for distinct sets $E, E' \in \mathcal{E}$. Namely, if there are distinct sets $E, E' \in \mathcal{E}$ with $E = \{y_1, y_2, y_3, y\}$ and $E' = \{y_1, y_2, y_3, z\}$, then for $q = 5^t$,

$$\begin{aligned} y_1y_2 + y_1y_3 + y_2y_3 + y \cdot (y_1 + y_2 + y_3) &\equiv 1 \bmod q \\ y_1y_2 + y_1y_3 + y_2y_3 + z \cdot (y_1 + y_2 + y_3) &\equiv 1 \bmod q \ . \end{aligned}$$

This implies

$$(y - z) \cdot (y_1 + y_2 + y_3) \equiv 0 \bmod 5^t \ .$$

As $(y_1 + y_2 + y_3) \not\equiv 0 \bmod 5$, we infer $y \equiv z \bmod q$, but we assumed that $E \neq E'$.
Now $|E \cap E'| \leq 2$ for distinct sets $E, E' \in \mathcal{E}$ implies that $x_4 \neq x_5$ and $x_3 \neq x_6$.
If we assume that $\mathcal{G}$ contains the configuration from above, then

$$x_3 \cdot (x_1 + x_2 + x_4) \equiv 1 - x_1x_2 - x_1x_4 - x_2x_4 \bmod q \tag{32}$$

$$x_3 \cdot (x_5 + x_7 + x_8) \equiv 1 - x_5x_7 - x_5x_8 - x_7x_8 \bmod q \tag{33}$$

$$x_6 \cdot (x_1 + x_2 + x_5) \equiv 1 - x_1x_2 - x_1x_5 - x_2x_5 \bmod q \tag{34}$$

$$x_6 \cdot (x_4 + x_7 + x_8) \equiv 1 - x_4x_7 - x_4x_8 - x_7x_8 \bmod q \ . \tag{35}$$

By multiplying po1 by po2 as well as po3 by po4, we obtain

$$\begin{aligned} & x_3 \cdot (1 - x_5x_7 - x_5x_8 - x_7x_8) \cdot (x_1 + x_2 + x_4) \\ \equiv\ & x_3 \cdot (x_5 + x_7 + x_8) \cdot (1 - x_1x_2 - x_1x_4 - x_2x_4) \bmod q \end{aligned} \tag{36}$$

$$\begin{aligned} & x_6 \cdot (1 - x_4x_7 - x_4x_8 - x_7x_8) \cdot (x_1 + x_2 + x_5) \\ \equiv\ & x_6 \cdot (x_4 + x_7 + x_8) \cdot (1 - x_1x_2 - x_1x_5 - x_2x_5) \bmod q \ . \end{aligned} \tag{37}$$

As $x_i \equiv 1 \bmod 5$, we can divide po5 by $x_3$, and po6 by $x_6$ without changing in the resulting congruence the modulus $q$. Evaluating po5 and po6, we infer

$$\begin{aligned} & x_1 + x_2 + x_4 - x_1x_5x_7 - x_1x_5x_8 - x_1x_7x_8 \\ & -x_2x_5x_7 - x_2x_5x_8 - x_2x_7x_8 - x_4x_5x_7 - x_4x_5x_8 - x_4x_7x_8 \\ \equiv\ & \\ & x_5 + x_7 + x_8 - x_5x_1x_2 - x_5x_1x_4 - x_5x_2x_4 \\ & -x_7x_1x_2 - x_7x_1x_4 - x_7x_2x_4 - x_8x_1x_2 - x_8x_1x_4 - x_8x_2x_4 \bmod q \end{aligned} \tag{38}$$

and

$$\begin{aligned} & x_4 + x_7 + x_8 - x_4x_1x_2 - x_4x_1x_5 - x_4x_2x_5 \\ & -x_7x_1x_2 - x_7x_1x_5 - x_7x_2x_5 - x_8x_1x_2 - x_8x_1x_5 - x_8x_2x_5 \\ \equiv\ & \\ & x_1 + x_2 + x_5 - x_1x_4x_7 - x_1x_4x_8 - x_1x_7x_8 \\ & -x_2x_4x_7 - x_2x_4x_8 - x_2x_7x_8 - x_5x_4x_7 - x_5x_4x_8 - x_5x_7x_8 \bmod q \ . \end{aligned} \tag{39}$$

Then we add po7 and po8, and we obtain

$$(x_4 - x_5) \cdot [2 - (x_1x_2 + x_7x_8) + 2 \cdot (x_1 + x_2) \cdot (x_7 + x_8)] \equiv 0 \bmod q \ . \tag{40}$$

Let $i$ be maximal such that $x_4 - x_5 \equiv 0 \bmod 5^i$. As $x_4 \neq x_5$, and $x_4, x_5 \in Z_{5^t}$, it follows that $i \leq t-1$. Then, dividing po9 by $(x_4 - x_5)$ yields

$$2 \cdot (x_1 + x_2) \cdot (x_7 + x_8) - x_1x_2 - x_7x_8 + 2 \equiv 0 \bmod 5 \ . \tag{41}$$

However, inserting $x_i \equiv 1 \bmod 5$ into po10 implies

$$2 \cdot 2 \cdot 2 - 1 \cdot 1 - 1 \cdot 1 + 2 \equiv 3 \not\equiv 0 \bmod 5 \ ,$$

which is a contradiction.
Moreover, we claim that $\mathcal{G}$ does not contain the following configuration:

$$\begin{aligned} A' &= \{x_2\} \cup \{x_1, x_3, x_4\} \\ B' &= \{x_2\} \cup \{x_3, x_5, x_8\} \\ C' &= \{x_2\} \cup \{x_1, x_5, x_6\} \\ D' &= \{x_2\} \cup \{x_4, x_6, x_8\} \ . \end{aligned}$$

This can be easily seen from the calculations from above, by setting in po1 - po10 $x_2$ equal to $x_7$. Since we did not divide by $x_2$ or $x_7$, the same conclusion follows.
Let us remark the following. Instead of defining the hypergraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, $\mathcal{E} \subseteq [\mathcal{V}]^4$ over the ring $Z_q$, we can define it over the field $GF(q)$. Namely, let $\mathcal{V} = GF(q)$ and let $\{x_1, \ldots, x_4\} \in \mathcal{E}$ if and only if

$$\begin{aligned} \sum_{1 \leq i < j \leq 4} x_i x_j &= c \\ \sum_{i \in I} x_i &\neq 0 \qquad\qquad \text{for all } I \in [\{1, \ldots, 4\}]^3 \end{aligned}$$

for a suitable $c \in GF(q)$, where $c$ is chosen such that $|\mathcal{E}| = \Theta(|\mathcal{V}|^3)$. By the results from [FF 86], $\mathcal{G}$ does not contain any configuration from $\mathcal{V}_1^{(4)}$. Thus, the strange thing happens, that dependent on whether we calculate in the field $GF(q)$ or in the ring $Z_q$, we exclude configurations from $\mathcal{V}_1^{(4)}$ and $\mathcal{V}_2^{(4)}$, respectively.

## 7 Acknowledgments

A part of this research was done when Pavel Pudlák visited Dortmund University as a Humboldt Fellow and when Petr Savický visited Dortmund University supported by Heinrich-Hertz-Stiftung grant number B42/44-93. We thank to Noga Alon for suggesting the method of conditional probabilities for derandomizing the proof of Theorem 2.3.

## References

[Ai 75] M. Aigner, Kombinatorik, Vol. I, Springer Verlag, Berlin, 1975.

[AGHP 92] N. Alon, O. Goldreich, J. Håstad and R. Peralta, Simple Constructions of Almost $k$-wise Independent Random Variables, *Random Structures & Algorithms* **3**, 1992, 289-304. Addendum: *Random Structures and Algorithms* **4**, 1993, 119-120.

[AS 92] N. Alon and J. Spencer, *The Probabilistic Method,* Wiley & Sons, New York, 1992.

[Be 66] C. T. Benson, Minimal Regular Graphs of Girth Eight and Twelve, *Canadian Journal of Mathematics* **18**, 1966, 1091-1094.

[BS 74] A. Bondy and M. Simonovits, Cycles of Even Length in Graphs, *Journal of Combinatorial Theory Ser. B* **16**, 1974, 97-105.

[Br 66] W. G. Brown, On Graphs that do not Contain a Thomasen Graph, *Canadian Mathematical Bulletin* **9**, 1966, 281-289.

[Ca 95] N. Calkin, Dependent Sets of Constant Weight Binary Vectors, *preprint,* 1995.

[Er 38] P. Erdős, On Sequences of Integers no One of which Divides the Product of Two Others and some Related Problems, *Izvestiya Nauchno-Issl. Inst. Mat. i Meh. Tomsk* **2**, 1938, 74-82. *Mitteilungen des Forschungsinstitutes für Math. und Mechanik*, Tomsk, in Zentralblatt **20**, 5.

[Er 59] P. Erdős, Graph Theory and Probability, *Canadian Journal on Mathematics* **11**, 1959, 34-38.

[ERS 66] P. Erdős, A. Rényi and V. T. Sós, On a Problem of Graph Theory, *Studia Scientiarum Mathematicarum Hungarica* **1**, 1966, 215-235.

[FF 86] P. Frankl and Z. Füredi, Union-Free Families of Sets and Equations over Fields, *Journal of Number Theory* **23**, 1986, 210-218.

[Fü 91] Z. Füredi, Turán Type Problems, *Surveys in Combinatorics,* London Math. Soc. LNS **166**, Cambridge University Press, (1991), 253-300.

[LUW 95] F. Lazebnik, V. A. Ustimenko, and A. J. Woldar, A New Series of Dense Graphs of High Girth, *Bulletin (New Series) of the American Mathematical Society* **32**, 1995, 73-79.

[LPR 93] H. Lefmann, K. T. Phelps and V. Rödl, Extremal Problems for Triple Systems, *Journal of Combinatorial Designs* **1**, 1993, 379-394.

[LPS 88] A. Lubotzky, R. Phillips and P. Sarnak, Ramanujan Graphs, *Combinatorica* **8**, 1988, 261-277.

[Ma 88] G. A. Margulis, Explicit Group Theoretical Construction of Combinatorial Schemes and Their Application to the Design of Expanders and Concentrators, *J. Probl. Inform. Transmission* **24**, 1988, 39-46.

[SS 94] M. Sipser and D. A. Spielman, Expander Codes, *Proc. 35-th FOCS*, 1994, 566-576.

[Sin 38] J. Singer, A Theorem in Finite Projective Geometry and Some Applications to Number Theory, *Transactions of the American Mathematical Society* **43**, 1938, 377-385.

[SEB 73] V. T. Sós, P. Erdős and W. G. Brown, On the Existence of Triangulated Spheres in 3-Graphs, and Related Problems, *Periodica Mathematica Hungarica* **3**, 1973, 221-228.

[Spi 95] D. A. Spielman, Linear-time Encodable and Decodable Error-correcting Codes, *Proc. 27-th STOC*, 1995, 388-397.

[Spi 95d] D. A. Spielman, Computationally Efficient Error-Correcting Codes and Holographic Proofs, PhD thesis, MIT, 1995.

[We 90] R. Wenger, Extremal Graphs with no $C_4$'s, $C_6$'s or $C_{10}$'s, *Journal of Combinatorial Theory Ser. B* **52**, 1991, 113-116.

# 8 Appendix

In the following table we compare the probabilistic lower bounds (3) with the best bounds which can be obtained from (5) for some small values of $k$ and $r$. Upper, resp. lower, rows show rounded exponents $x$ of the upper, resp. lower, bounds $O(m^x)$, resp. $\Omega(m^x)$, on $N(m,k,r)$. Except for $k=4$ and $r=2$ where the true value is $x=1.5$, all others are the best bounds that we know of. The table was computed by Petr Pudlák.

| k | 2 | $2^2$ | $2^3$ | $2^4$ | $2^5$ | $2^6$ |
|---|---|---|---|---|---|---|
| r=2 | 2 | 1.5 | 1.25 | 1.125 | 1.0625 | 1.03125 |
| | 2 | 1.33333 | 1.14286 | 1.06667 | 1.03226 | 1.01587 |
| 3 | 3 | 2 | 2 | 1.75 | 1.625 | 1.5625 |
| | 3 | 2 | 1.71429 | 1.6 | 1.54839 | 1.52381 |
| 4 | 4 | 3 | 2.5 | 2.25 | 2.125 | 2.0625 |
| | 4 | 2.66667 | 2.28571 | 2.13333 | 2.06452 | 2.03175 |
| 5 | 5 | 3.5 | 3 | 2.75 | 2.625 | 2.5625 |
| | 5 | 3.33333 | 2.85714 | 2.66667 | 2.58065 | 2.53968 |
| 6 | 6 | 4 | 3.5 | 3.25 | 3.125 | 3.0625 |
| | 6 | 4 | 3.42857 | 3.2 | 3.09677 | 3.04762 |
| 7 | 7 | 5 | 4 | 3.875 | 3.6875 | 3.59375 |
| | 7 | 4.66667 | 4 | 3.73333 | 3.6129 | 3.55556 |
| 8 | 8 | 5.5 | 4.75 | 4.375 | 4.1875 | 4.09375 |
| | 8 | 5.33333 | 4.57143 | 4.26667 | 4.12903 | 4.06349 |
| 9 | 9 | 6 | 5.25 | 5 | 4.75 | 4.625 |
| | 9 | 6 | 5.14286 | 4.8 | 4.64516 | 4.57143 |
| 10 | 10 | 7 | 6 | 5.5 | 5.25 | 5.125 |
| | 10 | 6.66667 | 5.71429 | 5.33333 | 5.16129 | 5.07937 |
| 11 | 11 | 7.5 | 6.5 | 6 | 5.75 | 5.625 |
| | 11 | 7.33333 | 6.28571 | 5.86667 | 5.67742 | 5.5873 |
| 12 | 12 | 8 | 7 | 6.5 | 6.25 | 6.125 |
| | 12 | 8 | 6.85714 | 6.4 | 6.19355 | 6.09524 |
| 13 | 13 | 9 | 7.5 | 7 | 6.75 | 6.625 |
| | 13 | 8.66667 | 7.42857 | 6.93333 | 6.70968 | 6.60317 |
| 14 | 14 | 9.5 | 8 | 7.5 | 7.25 | 7.125 |
| | 14 | 9.33333 | 8 | 7.46667 | 7.22581 | 7.11111 |
| 15 | 15 | 10 | 8.75 | 8 | 7.8125 | 7.65625 |
| | 15 | 10 | 8.57143 | 8 | 7.74194 | 7.61905 |
| 16 | 16 | 11 | 9.25 | 8.625 | 8.3125 | 8.15625 |
| | 16 | 10.66667 | 9.14286 | 8.53333 | 8.25806 | 8.12698 |