# On the power of two, three and four probes

Noga Alon * Uriel Feige †

December 4, 2008

**Abstract**

An adaptive $(n, m, s, t)$-scheme is a deterministic scheme for encoding a vector $X$ of $m$ bits with at most $n$ ones by a vector $Y$ of $s$ bits, so that any bit of $X$ can be determined by $t$ adaptive probes to $Y$. A non-adaptive $(n, m, s, t)$-scheme is defined analogously. The study of such schemes arises in the investigation of the static membership problem in the bitprobe model. Answering a question of Buhrman, Miltersen, Radhakrishnan and Venkatesh [SICOMP 2002] we present adaptive $(n, m, s, 2)$ schemes with $s < m$ for all $n$ satisfying $4n^2 + 4n < m$ and adaptive $(n, m, s, 2)$ schemes with $s = o(m)$ for all $n = o(\log m)$. We further show that there are adaptive $(n, m, s, 3)$-schemes with $s = o(m)$ for all $n = o(m)$, settling a problem of Radhakrishnan, Raman and Rao [ESA 2001], and prove that there are non-adaptive $(n, m, s, 4)$-schemes with $s = o(m)$ for all $n = o(m)$. Therefore, three adaptive probes or four non-adaptive probes already suffice to obtain a significant saving in space compared to the total length of the input vector. Lower bounds are discussed as well.

*Schools of Mathematics and Computer Science, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel and IAS, Princeton, NJ 08540, USA. Email: nogaa@tau.ac.il. Research supported in part by a USA Israeli BSF grant, by a grant from the Israel Science Foundation and by the Ambrose Monell Foundation.

†Department of Computer Science, the Weizmann Institute, Rehovot, Israel. Email: uriel.feige@weizmann.ac.il.

# 1 Introduction

In the study of the static membership problem in the bitprobe model, discussed in [10], [7] and [11], one needs to encode a vector $X$ of $m$ bits with at most $n$ ones by a vector $Y$ of $s$ bits such that any bit of $X$ can be determined by $t$ adaptive or non-adaptive probes to $Y$. Given $n, m$, and $t$ the objective is to minimize $s$. We consider here only deterministic algorithms with a small number of adaptive or non-adaptive probes. An adaptive $(n, m, s, t)$-scheme is a scheme for encoding a vector $X$ of $m$ bits with at most $n$ ones by a vector $Y$ of $s$ bits, so that any bit of $X$ can be determined by $t$ adaptive probes to $Y$. A non-adaptive $(n, m, s, t)$-scheme is defined analogously.

One motivation for the problem is as follows. There is a small set $Z$ of size $n$ which is part of a large universe $X$ of size $m$. For example, $Z$ may be the set of English words, and $X$ may be the set of all English character strings (up to a certain length). One needs to construct a space efficient data structure $Y$ (containing only $s$ bits) such that any membership query can be answered by inspecting at most $t$ bit locations in the data structure. (In the example above, $Y$ may be thought of as a dictionary by which one can tell whether a given character string is an English word or not.) The problem is static in the sense that there is no need to (efficiently) support insertion or deletion operations to and from $Z$. In this context it is instructive to consider the Bloom filter ([2], and see also a recent survey in [4]), which is a space-efficient data structure that allows one to answer membership queries by inspecting a small number of bit locations. It allows for efficient insertion operations, and in general requires less space than the constructions described in the current paper. However, this improved space efficiency of Bloom filters comes at the price of allowing false positives (though false positives are expected to happen only infrequently), whereas in this paper it is required that all queries are answered correctly. Other space efficient data structures that allow errors (with the frequency of errors controlled by using randomness in the data structure) are described in [7].

For deterministic error-free algorithms, it is easy to see that with one probe no space can be saved even if $n = 1$. That is, if an $(n, m, s, 1)$ scheme exists for some $m \geq 2$, $n \geq 1$, then $s \geq m$. Indeed, assuming $s < m$, there are $1 \leq i < j \leq m$ so that in order to determine $x_i$ or $x_j$ the algorithm probes the same bit of $Y$. As the two bits $x_i, x_j$ can attain at least three possible values when $n \geq 1$, it is impossible to distinguish between them using only one bit.

For the case $t = 1$ of one probe, the scheme is, of course, always non-adaptive. For 2-probes, there are already adaptive and non-adaptive schemes.

In [7] it is shown that with two non-adaptive probes, no space can be saved whenever $n \geq 2$. That is, if a non-adaptive $(2, m, s, 2)$-scheme exists, then $s \geq m$. On the other hand, the authors of [11] describe an adaptive $(2, m, O(m^{2/3}), 2)$-scheme (improving a proof of existence of an adaptive $(2, m, O(m^{3/4}), 2)$-scheme given in [7]). Thus, if $n = 2$, then a second adaptive probe can help to reduce the space below $m$. The authors of [7] mention that they do not know if any space can be saved with two adaptive probes when $n > 2$. The following two results show that indeed some space can be saved as long as $n$ is not too large.

**Theorem 1.1** *For every $m \geq n$ there are adaptive $(n, m, s, 2)$-schemes with $s \leq m - \frac{m}{2n+2} + 2n$. Thus, $s < m$ provided $m > 4n^2 + 4n$.*

We do not know whether space can be saved if $m < 4n^2$. If $n$ is smaller, however, more space can be saved.

**Theorem 1.2** *For $n < \log m$ there is an adaptive $(n, m, s, 2)$-scheme with*

$$s \leq O(\frac{mn \log[\frac{\log m}{n}]}{\log m}).$$

*Thus, $s = o(m)$ whenever $n = o(\log m)$.*

A general lower bound for the space in adaptive schemes is proved in [7]; it is shown that if an adaptive (or non-adaptive) $(n, m, s, t)$-scheme exists, then $s \geq \Omega(tn^{1-1/t}m^{1/t})$. (The lower bound quoted there is $ntm^{\Omega(1/t)}$, but the proof gives the previous estimate, which implies the last one only for $n < m^{1-\delta}$. The last estimate is, in fact, not valid for $n$ close to $m$.) In particular, for 2-adaptive probes the lower bound for the space is $\Omega(n^{1/2}m^{1/2})$.

For three adaptive (or non-adaptive) probes, the lower bound of [7] is $\Omega(n^{2/3}m^{1/3})$. We obtain a better lower bound for the non-adaptive case.

**Theorem 1.3** *If a non-adaptive $(n, m, s, 3)$-scheme exists and $n \geq 16 \log m$, then*

$$s \geq \Omega(n^{1/2}m^{1/2}/\log^{1/2} m).$$

We show that with three adaptive probes, the space can be much smaller than $m$ whenever $n$ is significantly smaller than $m$.

**Theorem 1.4** *For all $n \leq m$, there are adaptive $(n, m, s, 3)$-schemes with $s \leq O(n^{1/3}m^{2/3})$. Thus, the space is $o(m)$ whenever $n = o(m)$.*

Note that the trivial information theoretic lower bound gives that even if the algorithm is allowed to read all the vector $Y$ in order to recover any desired bit of $X$, then $s$ must still be at least $\log(\sum_{i \leq n} \binom{m}{i})$. Thus, if one hopes to achieve $s = o(m)$, then $n$ must be $o(m)$ even if the number of probes is unlimited. Remarkably, by Theorem 1.4 three adaptive probes already suffice to achieve a saving of this type. This disproves a conjecture of [11].

A similar pattern of saving in space can be obtained by four non-adaptive probes.

**Theorem 1.5** *For all $n \leq m$, there are non-adaptive $(n, m, s, 4)$-schemes with $s \leq O(n^{1/4}m^{3/4})$. Thus, $s = o(m)$ provided $n = o(m)$.*

This improves (in two respects) a result of [7] asserting that 5 non-adaptive probes suffice to get space $s = o(m)$ whenever $n = o(m^{1/3})$.

The rest of this paper is organized as follows. In Section $i$, for $2 \leq i \leq 4$, we discuss schemes with $i$ probes. The final Section 5 contains some open problems, among them issues relating to explicitly constructing the schemes guaranteed to exist by theorems 1.4 and 1.5. Throughout the paper we make no attempt to optimize the absolute constants hidden in the $O$ notation. To simplify the presentation, we omit all floor and ceiling signs whenever these are not crucial. All logarithms are in base 2, unless otherwise specified.

## 2 Two Probes

**Proof of Theorem 1.1**

For simplicity we assume that $2n + 2$ divides $m$. The encoding is as follows.

We arrange $X$ in $2n+2$ consecutive columns, each of length $m/(2n+2)$. There must be a pair of adjacent identical columns, so collapse them to one column, moving all subsequent columns one location to the left. For each column (except for the first and last one), add one bit that says whether it stayed in place or was shifted left.

To read a bit of $X$, first probe the corresponding column bit, and then use the answer to decide which column to probe (at the appropriate bit location). □

**Proof of Theorem 1.2**

Let $G = (V, E)$ be a connected, $d$-regular bipartite graph on $s$ vertices with $2m$ edges, and girth $g$ bigger than $\frac{\log s}{\log d} = \frac{\log s}{\log(4m/s)}$, where $d$ is even. There are several known explicit constructions of such graphs, see, for example, [9] and its references. (For simplicity we assume that the number of edges is precisely $2m$; if there is no construction with these precise parameters there is no problem to take a subgraph of a slightly bigger graph instead). Let $A = \{1, 2, \ldots, s/2\}$ and $B = \{s/2+1, \ldots, s\}$ denote the classes of vertices of $G$. By partitioning the edges incident with each vertex of $A$ into disjoint pairs we get a partition of all edges of $G$ into $m$ pairwise edge-disjoint paths of length 2 whose centers lie in $A$. Fix such a partition into $m$ paths $P_1, \ldots, P_m$. For each $i$, $1 \leq i \leq m$, denote the vertices of $P_i$ by $\{a_i, b_i, c_i\}$, where $a_i \in A$ and $b_i, c_i \in B$. Our scheme encodes the vector $X = (x_1, x_2, \ldots, x_m)$ by the vector $Y = (y_1, y_2, \ldots, y_s)$ so that for every $i$, the value of $x_i$ can be recovered by two adaptive probes to $Y$ as follows: if $y_{a_i} = 0$ then $x_i = y_{b_i}$, and if $y_{a_i} = 1$, then $x_i = y_{c_i}$. Therefore, in order to determine the value of $x_i$ one first probes $y_{a_i}$, and depending on its value, proceeds to probe either $y_{b_i}$ or $y_{c_i}$. We claim that if the girth $g$ and the parameters $n, m, s$ satisfy

$$g > \frac{\log s}{\log(4m/s)} \geq \frac{16mn}{s} \tag{1}$$

then any vector $X$ with at most $n$ ones can be encoded in a way that supports the above decoding. Observe, first, that the Boolean function $f = f(z_1, z_2, z_3)$ defined by $f(z_1, z_2, z_3) = z_{f(z_1)+2}$ has the property that given control of any two of its three input bits $z_1, z_2, z_3$ enables one to control the output. Indeed, if the desired output is $b$ and the two given input bits are $z_2, z_3$, set $z_2 = z_3 = b$, if the two given input bits are $z_1, z_2$ then set $z_1 = 0$ and $z_2 = b$ and, symmetrically, if the two given bits are $z_1, z_3$ set $z_1 = 1$ and $z_3 = b$. Note that in order to get $b$ as an output one never has to set any of the given bits among the two bits $z_2, z_3$ to $1 - b$.

In our scheme, $x_i$ should be $f(y_{a_i}, y_{b_i}, y_{c_i})$ for every $i$. Call a location $i$ in $X$ a 1-bit if $x_i = 1$. Call a location $j$ in $X$ intersecting if $x_j = 0$ and the set $\{b_j, c_j\}$ intersects the union $\cup_{i:x_i=1}\{b_i, c_i\}$. The encoding scheme will assign to each 1-bit and each intersecting bit $x_i$ two of the three bits $y_{a_i}, y_{b_i}, y_{c_i}$, and this will be done so that no bit of $Y$ will be assigned more than once. This will enable us to determine the values of the assigned bits of $Y$ in order to ensure that each of the 1-bits and intersecting bits of $X$ will indeed be recovered correctly by two adaptive probes to $Y$. Moreover, as explained above, the only bits of $Y$ that are set to 1 in this process are some of the bits $y_i$ with $i \in A$ and some of the bits $y_j$ with $j \in \cup_{i:x_i=1}\{b_i, c_i\}$. Setting all remaining bits of $Y$ to zero will now ensure that all bits of $X$ can be recovered correctly. It remains to show that we can assign two bits of $Y$ as above to each of the 1-bits and intersecting bits of $X$, as needed. By Hall's Theorem, this is equivalent to showing that for every subset $I$ of locations of such bits, the cardinality of the union $\cup_{i \in I}\{a_i, b_i, c_i\}$ is at least $2|I|$.

By assumption, the number of 1-bits in $X$ is at most $n$. Therefore, $|\cup_{i,x_i=1}\{b_i, c_i\}| \leq 2n$ and hence the number of intersecting bits is at most $(d-1)2n$. It follows that the sets $I$ we have to

consider are of cardinality at most $2nd$. For each such set, the number of edges in the union of all paths $P_i$ for $i \in I$ is exactly $2|I| \leq 4nd = \frac{16mn}{s}$, which is smaller than the girth of the graph $G$, by the assumption (1). Therefore, the subgraph consisting of all these edges is a forest, and hence its number of vertices exceeds its number of edges, which is $2|I|$. The desired result thus follows by Hall's Theorem. To complete the proof observe that the smallest $s$ satisfying (1) is indeed $O(\frac{mn \log[\log m/n]}{\log m})$. Note that the last quantity is $O(\frac{m \log f}{f})$, where $f = \frac{\log m}{n}$, and thus $s = o(m)$ provided $n = o(\log m)$. $\Box$

It is interesting to note that Theorem 6 in [11] asserts that under certain conditions (that are satisfied by the schemes described therein), when $n \geq 3$ then $s \geq m$. Hence our two schemes above show the advantage of deviating from these conditions.

# 3 Three Probes

## 3.1 The lower bound for three non-adaptive probes

There is a simple proof of a lower bound of $s \geq \Omega(m^{1/3}n^{2/3})$. Although this lower bound is not very impressive, as Theorem 6 in [7] gives essentially the same bound for three adaptive probes, we describe this proof, since our improved result starts with the same basic approach.

Any non-adaptive $(n, m, s, 3)$-scheme can be described by a collection of $m$ triples of bits of $Y$, together with $m$ functions of these triples that give the bits of $X$. Given such a scheme, choose at random $n-1$ out of the $s$ bits of $Y$. Then (in expectation, and hence for some choice) $g \geq m(n/s)^3$ of the triples are contained in them (up to a negligible error). If $g \geq n$ then $Y$ cannot encode $X$. Thus $m(\frac{n}{s})^3 \leq (1 + o(1))n$, implying $s \geq \Omega(m^{1/3}n^{2/3})$, as claimed.

The above argument suggests the study of the following extremal problem for hypergraphs. The notation is somewhat non-standard for hypergraphs, but is chosen so as to be consistent with that of the probes model. Let $H(s, n)$ be the maximum number of hyperedges that an $s$ vertex 3-uniform hypergraph can contain without including a set of $g < n$ vertices that induces more than $g$ hyperedges. If $m > H(s, n)$, then an $m$ bit string with at most $n$ ones cannot be encoded by $s$ bits in the nonadaptive three probe setting.

Note that for a random 3-uniform hypergraph (3-graph, for short) and $n \geq \log s$, we get that $H(s, n) = \Omega(s^2/n)$. This follows from a simple probabilistic argument, and the fact that for $m = cs^2/n$, with $c$ a sufficiently small constant,

$$\sum_{g<n} \binom{s}{g} \binom{m}{g+1} (g/s)^{3g+3} < 1.$$

We also note that a closely related problem to that of determining or estimating $H(s, n)$ has been considered before, but for a very different choice of parameters dealing mainly with cases of more vertices than edges in the forbidden substructure. See [1], [5], [6], [12], [13]. These results and proof techniques do not seem useful here, and we need a different argument.

Our objective is to show that for $n \geq \Omega(\log s)$ the $\Omega(s^2/n)$ lower bound is tight, up to a logarithmic factor. Note that this is not the case for small values of $n$, in fact, for fixed $n$ even the probabilistic construction described above yields a better than $\Omega(s^2)$ lower bound, namely an $\Omega(s^{2+1/n})$ lower bound. In several cases one can give a better explicit bound. As a particular example, $H(s, 7) \geq \Omega(s^{5/2})$ as shown by the 3-uniform hypergraph obtained by taking 3 disjoint

sets of vertices $A, B, C$, each of size $s/3$, taking the incidence graph $F$ of the points and lines of a projective plane on $A$ and $B$, which is a graph with $\Omega(s^{3/2})$ edges and girth 6, and considering the 3-graph consisting of all edges that are a union of an edge of the graph $F$ with a vertex of $C$.

We proceed with the proof of the upper bound for $H(s,n)$. We need two simple lemmas for (multi)-graphs (usual 2-graphs, possibly with multiple edges).

**Lemma 3.1** *Every graph with $s$ vertices and more than $3s$ edges contains a set of $k \leq 4\log s$ vertices which spans at least $k+1$ edges.*

**Proof:** It is well known that every graph with $s$ vertices and at least $2s$ edges contains a cycle of length at most $2\log s$. Take such a cycle $C_1$, omit its edges, and repeat. As long as there are at least $2s$ edges remaining, we can find another cycle, thus the process terminates with a collection of pairwise edge-disjoint cycles, each of length at most $2\log s$, so that their total length exceeds $s$. Thus two of the cycles share a common vertex, and their union provides the required result. □

**Lemma 3.2** *For $s \geq n \geq 8\log s$, any graph with $s$ vertices and at least $3s + n/2$ edges contains a set of $k \leq n/2$ vertices spanning at least $k + \frac{n}{8\log s}$ edges.*

**Proof:** Starting with an empty set of vertices $X$, apply Lemma 3.1 to find a set of vertices $K_1$ of $k_1 \leq 4\log s$ vertices spanning at least $k_1 + 1$ edges. Add those vertices to $X$, omit the edges and apply Lemma 3.1 again to find another such set $K_2$, add it to $X$ and omit its edges. Continuing in this manner $n/(8\log s)$ steps we get the desired result. □

We can now prove the following for 3-graphs, showing that for all $s \geq n \geq 16\log s$,

$$H(s,n) \leq O(s^2 \log s/n).$$

**Lemma 3.3** *Suppose $s \geq n \geq 16\log s$. Then any 3-graph $H$ with $s$ vertices and $m \geq \frac{11s^2\log s}{n}$ edges contains a set of $g < n$ vertices with at least $g+1$ edges.*

**Proof:** Let $U$ be a set of $\frac{n}{9\log s}$ vertices chosen by the following greedy iterative procedure. Initially all hyperedges are not marked and $U$ is empty. In every step add to $U$ the vertex contained in the largest number of unmarked hyperedges of $H$ (breaking ties arbitrarily), and mark these hyperedges. The total number of hyperedges marked in the process of selecting $U$ is at least roughly $\frac{3|U|}{s}m = \frac{mn}{3s\log s}$ (up to a multiplicative term of $(1+O(\frac{|U|}{s}))$ that tends to 1 as $s$ grows). This can be seen by observing that the fraction of unmarked hyperedges is at most $\left(\frac{s-|U|}{s}\right)^3 \leq 1 - \frac{3|U|}{s} + \frac{3|U|^2}{s^2}$, which would be an upper bound on their fraction had $U$ been chosen randomly. Let $G$ be the (multi)-graph on the set of vertices of $H$ whose edges are all edges of the form $e - \{u\}$ where $e$ is a marked hyperedge of $H$ and $u \in U$ is the vertex who caused $e$ to be marked. Then $G$ has $s$ vertices and at least $\frac{mn}{3s\log s}$ edges. If this exceeds $3.5s \geq 3s + n/2$ then, by Lemma 3.2, there is a set $W$ of $k \leq n/2$ vertices of $G$ which spans at least $k + \frac{n}{8\log s}$ edges of $G$. The union $U \cup W$ thus contains $g \leq k + \frac{n}{9\log s} < n$ vertices and at least $k + \frac{n}{8\log s} > g$ edges. □

Note that the proof also provides a deterministic efficient algorithm for finding, given a 3-graph with $s$ vertices and at least $11s^2\log s/n$ edges, a set of at most $n$ edges whose characteristic vectors are not linearly independent.

**Proof of Theorem 1.3.** If a non-adaptive $(n, m, s, 3)$ scheme exists then $m \leq H(s, n)$, as explained in the beginning of this subsection. Therefore, by Lemma 3.3, $m \leq O(s^2 \log s/n)$, supplying the desired lower bound for $s$. $\Box$

### 3.2 A scheme with 3 adaptive probes

In this subsection we prove Theorem 1.4. The scheme is a natural extension of the one for two probes, described in the previous section. Each bit of $X$ here will be recovered by probing two bits of $Y$ in order to select one of four possible bits of $Y$. Let $F(z_1, z_2, \ldots, z_6)$ be the Boolean function of 6 input bits defined by $F(z_1, z_2, \ldots, z_6) = z_{3+2z_2+z_1}$. It is to check the following.

**Claim 3.4** *For any set $I \subset \{1, 2, \ldots, 6\}$ of cardinality 4, and for any value $b \in \{0, 1\}$, one can set the values of the bits $z_i$ for $i \in I$ so that for any values of the bits $z_i$, $i \in \{1, 2, \ldots, 6\} - I$, $F(z_1, z_2, \ldots, z_6) = b$. Moreover, this can be done by assigning all bits in the set $I \cap \{3, 4, 5, 6\}$ the value $b$.*

Indeed, if $I = \{3, 4, 5, 6\}$ then we set $z_3 = z_4 = z_5 = z_6 = b$. If $I$ contains both numbers $1, 2$ then it also contains an additional number (in fact, two additional numbers). Let the smallest among them be $3+2w_2+w_1$ where $w_1, w_2 \in \{0, 1\}$, and set $z_1 = w_1, z_2 = w_2$ and $z_{3+2w_2+w_1} = b$. If $I$ contains only one of the numbers $1, 2$, say 1, then it also contains either the two numbers $z_3, z_5$ or the two numbers $z_4, z_6$. In the first case set $z_1 = 0$ and $z_3 = z_5 = b$, and in the second $z_1 = 1$ and $z_4 = z_6 = b$. The case $I \cap \{1, 2\} = \{2\}$ is symmetric. This proves the claim.

For each bit $x_i$ of $X$ our scheme will have six locations in $Y$, that is, a set $A_i$ of six numbers $a_{i1} < a_{i2} < \ldots < a_{i6}$, where $a_{i1}, a_{i2} \in A = \{1, 2, \ldots, s/3\}$ and $a_{i3}, \ldots, a_{i6} \in B = \{s/3+1, \ldots, s\}$. The encoding will ensure that for each $i$, $x_i = F(y_{a_{i1}}, y_{a_{i2}}, \ldots, y_{a_{i6}})$. In order to enable such an encoding, the sets $A_i$ will have to satisfy a certain expansion property. The existence of such sets is proved in the next lemma.

**Lemma 3.5** *There exists an absolute constant $c$ so that for every $m \geq n, s$ and $d$ that satisfy $s \geq cm^{2/3}n^{1/3}$, $6m = ds$ there is a bipartite (multi)-graph $G$ with the following properties.*
*(i) The classes of vertices of $G$ are $U$ and $W = A \cup B$, where $|U| = m$, $|A| = s/3$, $|B| = 2s/3$ and $A \cap B = \emptyset$.*
*(ii) Every vertex $u \in U$ has exactly 2 neighbors in $A$ and exactly 4 neighbors in $B$, and the degree if every vertex of $W$ is exactly $d$.*
*(iii) Every set $R \subset U$ satisfying $|R| \leq 4nd = 24mn/s$ has more than $4|R|$ neighbors in $W$.*

**Proof**: The proof is probabilistic, applying (a slight variant of) the configuration model described, for example, in [3]. Let $U', A', B'$ be disjoint sets of sizes $|U'| = 6m, |A'| = sd/3, |B'| = 2sd/3$, and suppose that $U'$ is partitioned into $m$ groups, each of size 6, $A'$ is partitioned into $s/3$ groups, each of size $d$, and $B'$ is partitioned into $2s/3$ groups, each of size $d$. Let $\pi$ be a random perfect matching $M$ between the elements of $U'$ and those of $W' = A' \cup B'$, chosen uniformly among all $(2m)!(4m)!$ matchings that match the $2m$ members of $U'$ consisting of the first two elements of each group with the members of $A'$ and the remaining $4m$ members of $U'$ with those of $B'$. The graph $G$ is obtained by collapsing each group into a single vertex, thus getting a bipartite graph with classes of vertices $U$ and $W = A \cup B$. Each matching edge $u'w'$, with $u' \in U'$ and $w' \in W' = A' \cup B'$ becomes an edge $uw$ of $G$, where $u$ is the vertex corresponding

to the group containing $u'$, and $w$ is the vertex corresponding to the group containing $w'$. Thus $|U| = m$, $W$ is the disjoint union of $A$ and $B$ where $|A| = s/3$ and $|B| = 2s/3$, the degree of every vertex of $U$ is 6, and that of every vertex of $W = A \cup B$ is $d$. Therefore, $G$ satisfies properties (i) and (ii). Note that it may well have parallel edges.

It remains to show that with positive probability, property (iii) holds. To do so, we bound the probability that there is some $r \leq 24mn/s$ and a set $R$ of $r$ vertices in $U$ that has at most $4r$ neighbors in $W$. For a fixed $r$, there are $\binom{m}{r}$ possibilities to pick a set $R$ of $r$ vertices in $U$, and $\binom{s}{4r}$ possibilities to pick a set of $T$ of $4r$ vertices in $W$. Fix such two sets $R$ and $T$. Let $R'$ denote the set of $6r$ members of $U'$ that lie in the groups that form the vertices in $R$, and let $T'$ denote the set of $4rd$ members of $W'$ that lie in the groups that form the vertices of $T$. The probability that all neighbors of the vertices of $R$ lie in $T$ is the probability that the random matching picked in the definition of $G$ matched all $6r$ members of $R'$ to some $6r$ elements in $T'$. There are at most $4rd(4rd-1)\ldots(4rd-6r+1)$ ways to match the members of $R'$ to $6r$ elements of $T'$. (This is an overcount, as some of these matchings may be impossible, since the matching matches exactly two elements in every group of six to members of $A'$. Still, the above estimate suffices for our purpose here.) The total number of choices for the matching edges containing the elements of $R'$ is precisely

$$|A'|(|A'|-1)\cdots(|A'|-2r+1)|B'|(|B'|-1)\cdots(|B'|-4r+1)$$
$$= \frac{sd}{3}(\frac{sd}{3}-1)\cdots(\frac{sd}{3}-2r+1)\frac{2sd}{3}(\frac{2sd}{3}-1)\cdots(\frac{2sd}{3}-4r+1).$$

Thus, the probability that all members of $R'$ are matched to members of $T'$ is at most the ratio between these two quantities, which is at most

$$(\frac{4rd}{sd/3})^{2r}(\frac{4rd}{2sd/3})^{4r} = (c_1 r/s)^{6r},$$

for some absolute constant $c_1$. It follows that the probability that there is some $r \leq 24mn/s$ and a subset $R \subset U$ of cardinality $r$ with at most $4r$ neighbors is at most

$$\sum_{r=1}^{24mn/s}\binom{m}{r}\binom{s}{4r}(c_1 r/s)^{6r} \leq \sum_{r=1}^{24mn/s}(c_2\frac{m}{r}(\frac{s}{r})^4(\frac{r}{s})^6)^r = \sum_{r=1}^{24mn/s}(c_2\frac{mr}{s^2})^r,$$

for some absolute constant $c_2$. For $r \leq 24mn/s$, the quantity $c_2\frac{mr}{s^2}$ is smaller than $1/2$, provided $s$ is at least $cm^{2/3}n^{1/3}$ for an appropriately chosen absolute constant $c$. Thus, for such an $s$, the probability that (iii) does not hold is smaller than $\sum_{r=1}^{24mn/s}(1/2)^r < 1$, and therefore there exists a bipartite graph as needed. □

**Proof of Theorem 1.4:** Given $m \geq n$, let $s = cm^{2/3}n^{1/3}$ satisfy the assumptions of Lemma 3.5, and put $d = 6m/s$. Let $G$ be a bipartite multigraph with classes of vertices $U = \{u_1, u_2, \ldots, u_m\}$ and $W = A \cup B$, where $A = \{1, 2, \ldots, s/3\}$ and $B = \{s/3+1, \ldots, s\}$, satisfying the conclusions of the lemma. For each $i$, $1 \leq i \leq m$, let $A_i$ be the set of neighbors of $u_i$ in $W$. Note that if there are no parallel edges incident with $u_i$, then $A_i$ contains exactly 2 members of $A$ and 4 of $B$. Otherwise, there is only one such parallel edge (by applying the condition (iii) with $|R| = 1$). In this case add to $A_i$ an arbitrary additional member of $\{1, 2, \ldots, s\}$ to ensure that the modified set consists of exactly 2 members of $A$ and 4 of $B$, and call this element

the exceptional member of $A_i$. We now show that the sets $A_i$ enable us to encode any given vector $X = (x_1, \ldots, x_m)$ with at most $n$ ones by a vector $Y$, using the scheme described in the paragraph preceding Lemma 3.5. As in the proof of Theorem 1.2, call a location $i$ in the vector $X$ a 1-bit if $x_i = 1$, and call a location $j$ an intersecting bit if $x_j = 0$ and the set of non-exceptional positions among $a_{j3}, a_{j4}, a_{j5}, a_{j6}$ intersects the set of all non-exceptional elements in $\cup_{i:x_i=1}\{a_{i3}, a_{i4}, a_{i5}, a_{i6}\}$. Since each number $k \in B$ serves as a non-exceptional position of exactly $d = 6m/s$ sets, it follows that the number of intersecting bits is at most $4n(d-1)$ and hence the total number of 1-bits and intersecting bits is at most $4nd = 24mn/s$. By Hall's Theorem and the properties of the graph $G$ we can assign to each 1-bit or intersecting bit $i$ four non-exceptional positions in $A_i$, so that no position is assigned more than once. We can now complete the encoding using the properties in Claim 3.4, by using the four assigned locations to encode the 1-bits and intersecting bits, and by setting all other bits of $Y$ to zero. This completes the proof. □

# 4 Four Probes

In this section we prove Theorem 1.5. The proof extends an approach of [7].

**Definition 4.1** *Let $G$ be an $r$-uniform hypergraph in which every hyperedge is either labelled as a 1-edge or a 0-edge, and let $p, q$ be integers with $0 < q \leq p < r$. In the $(p, q)$-coloring problem, one needs to color the vertices of the hypergraph by 1/0 such that every 1-edge has at least $p$ vertices colored 1, and every 0-edge has at least $q$ vertices colored 0.*

The $(p, q)$-coloring problem is NP-hard. In particular, it generalizes the usual notion of two coloring of uniform hypergraphs (set $p = q = 1$ and make two copies of every hyperedge, one as a 1-edge and the other as a 0-edge). We provide sufficient conditions on the expansion of $G$ that ensure the existence of a $(p, q)$-coloring, regardless of which are the 1-edges and which are the 0-edges.

**Definition 4.2** *We say that a hypergraph has expansion $\alpha$ if every set $E$ of hyperedges spans at least $\alpha|E|$ vertices.*

The key to our non-adaptive $(n, m, s, 4)$-scheme is the following lemma, whose proof appears in Section 4.1.

**Lemma 4.1** *Let $G$ be an arbitrary 4-uniform hypergraph with $s$ vertices and $m$ hyperedges, for which every set of $2n$ hyperedges induces a subhypergraph with expansion $\alpha \geq 8/3$. Then for any choice of at most $n$ hyperedges, labelling the chosen hyperedges as 1-edges and the remaining hyperedges as 0-edges, the resulting labelled hypergraph has a legal $(3, 2)$-coloring. Moreover, such a coloring can be found in polynomial time.*

Given a hypergraph $G$ as in Lemma 4.1 we obtain a non-adaptive $(n, m, s, 4)$-scheme as follows. Every bit $x_i$ of the encoded vector $X = \{x_1, \ldots, x_m\}$ is associated with a hyperedge $E_i$. Every bit $y_j$ of the encoding vector $Y = \{y_1, \ldots, y_s\}$ is associated with a vertex $v_j$. To decode the value of a bit $x_i$, probe the four bits of $Y$ that correspond to the vertices in the respective hyperedge $E_i$. If $\sum_{v_j \in E_i} y_j \geq 3$ then $x_i = 1$, and if $\sum_{v_j \in E_i} y_j \leq 2$ then $x_i = 0$. If follows that

an encoding of $X$ is precisely a legal $(3,2)$-coloring of $G$. Such a legal coloring is needed only when the number of ones in $X$ is at most $n$, and Lemma 4.1 provides a sufficient condition for such a legal coloring to exist.

Lemma 4.2 (with a choice of $\delta \leq 1/3$) implies that hypergraphs $G$ with expansion properties as needed in Lemma 4.1 exist with parameters as stated by Theorem 1.5. Note that Lemma 4.2 is stated in terms of bipartite graphs, but these bipartite graphs can naturally be viewed as 4-uniform hypergraphs with $W$ as the set of vertices of the hypergraph and $U$ as the set of hyperedges.

**Lemma 4.2** *There exists an absolute constant $c > 0$, so that for every $\delta > 0$ and every $m > n$ and $s$ that satisfy $s \geq cm^{1/(1+\delta)}n^{\delta/(1+\delta)}$ there is a bipartite graph $G$ with classes of vertices $U$ and $W$ and the following properties.*
*(i) $|U| = m$ and $|W| = s$.*
*(ii) Every vertex of $U$ has degree 4.*
*(iii) Every set $R$ of $r \leq 2n$ vertices of $U$ has more than $(3-\delta)r$ neighbors in $W$.*

**Proof**: The proof is probabilistic, and is simpler than that of Lemma 3.5 as here there are no constraints on the degrees of the vertices of $W$. Let $U$ and $W$ be disjoint sets with $|U| = m, |W| = s$, and let $G$ be the random graph obtained by picking, for each vertex $u \in U$ randomly and independently, a set $A_u \subset W$ of four distinct neighbors, where all 4-sets are taken with equal probability. Clearly $G$ satisfies conditions (i) and (ii), and it remains to show that it satisfies (iii) with positive probability. The expected number of sets $R$ that violate (iii) is at most

$$\sum_{1\leq r\leq 2n}\binom{m}{r}\binom{s}{\lfloor(3-\delta)r\rfloor}[\frac{\binom{\lfloor(3-\delta)r\rfloor}{4}}{\binom{s}{4}}]^r \leq \sum_{1\leq r\leq 2n}[\frac{em}{r}(\frac{es}{(3-\delta)r})^{3-\delta}(\frac{(3-\delta)r}{s})^4]^r$$

$$\leq \sum_{1\leq r\leq 2n}[c_1\frac{ms^{3-\delta}r^4}{r^{4-\delta}s^4}]^r = \sum_{1\leq r\leq 2n}[c_1\frac{mr^\delta}{s^{1+\delta}}]^r$$

$$\leq \sum_{1\leq r\leq 2n}[c_2\frac{mn^\delta}{s^{1+\delta}}]^r,$$

where $c_1, c_2 > 0$ are absolute constants. If $s \geq c_3 m^{1/(1+\delta)}n^{\delta/(1+\delta)}$ for an appropriately chosen $c_3$ (as a function of $c_2$), the term in the brackets is smaller than $1/2$ and hence the sum is smaller than 1, showing that with positive probability there are no sets $R$ violating condition (iii). □

As explained above, the combination of Lemmas 4.1 and 4.2 proves Theorem 1.5. Hence it remains to prove Lemma 4.1, which is the topic of the following section.

## 4.1 Expansion implies coloring of hypergraphs

The notion of $(p,q)$-coloring corresponds to an encoding scheme whenever $p + q > r$. Then a legal $(p,q)$-coloring uniquely determines which are the 1-edges and which are the 0-edges. The non-adaptive $(n,m,s,5)$-scheme of [7] may be viewed as based on $(3,3)$-colorings of 5-uniform hypergraphs. When $r$ is odd and $p = q = \frac{r+1}{2}$, then an expansion of $\alpha \geq p = q$ is a best possible sufficient condition for a $(p,q)$-coloring. (By Hall's condition, there is a matching that matches

$\frac{r+1}{2}$ vertices to every hyperedge, and these vertices can be colored by the color preferred by the hyper-edge. Tightness is demonstrated by the following example. There are $n$ 1-edges each with one unshared vertex, $n$ 0-edges each with one unshared vertex, and $n(r-1)$ additional vertices shared by the 1-edges and 0-edges. Adding one 0-edge that contains $\frac{r+1}{2}$ of the unshared vertices associated with 1-edges and $\frac{r-1}{2}$ additional fresh vertices, there is no legal $(p,q)$-coloring.) We shall be interested in the case that $r$ is even, namely, $r=4$, $p=1+r/2=3$ and $q=r/2=2$. As above, Hall's condition implies that an expansion of $\alpha=3$ suffices in order to guarantee a $(3,2)$ coloring. We show that a smaller expansion also suffices.

**Theorem 4.3** *Every 4-uniform hypergraph $G$ with expansion $\alpha=8/3$ is $(3,2)$-colorable, and 8/3 is the smallest possible value of $\alpha$ that guarantees a $(3,2)$-coloring.*

The following infinite family of examples proves the second part of Theorem 4.3, namely, that an expansion of 8/3 is necessary in order to guarantee $(3,2)$-coloring of 4-uniform hypergraphs. Let $k$ be arbitrarily large. Let there be $4k$ disjoint 1-edges, numbered 0 to $4k-1$. Cover $8k$ of their vertices by $2k$ disjoint 0-edges as follows. 0-edge $i$ for $0 \leq i \leq k-1$ contains one vertex from each of the 1-edges $4i, 4i+1, 4i+2, 4i+3$. 0-edge $k+i$ contains one (different) vertex from 1-edges $4i+2, 4i+3, 4i+4, 4i+5$ (where addition is performed modulo $2k$). Observe that this gives $6k$ edges, $16k$ vertices, and expansion 8/3. Every legal $(3,2)$-coloring must color $4k$ of the shared vertices by the color 0, and hence all remaining vertices by the color 1. Now, add one more 0-edge spanning three of the unshared vertices (say, belonging to 1-edges $k, 2k$ and $3k$), and one more fresh vertex. The expansion drops to $8/3 - O(1/k)$, and the resulting hypergraph is not $(3,2)$-colorable.

The more interesting part of the proof of Theorem 4.3 is to show that an expansion of 8/3 suffices. Similar to the case of odd $r$, a straightforward matching argument shows that an expansion of $\alpha=3$ suffices. As a warmup towards our main result, we now show that any value of $\alpha > 14/5$ suffices. Our proof is based on the following *trivial algorithm*. Initially, all vertices are uncolored and all edges are *active*. In every step of the algorithm, either (at least) one uncolored vertex gets colored, or (at least) one active edge becomes legally colored and drops out of the set of active edges. Let us explain these basic steps in more details. A vertex becomes colored 1 if there is no active 0-edge that contains it. Likewise, a vertex becomes colored 0 if there is no active 1-edge that contains it. (If some vertex is not in any active edge, it can be colored arbitrarily.) Observe that for an active edge, all its vertices are either uncolored, or colored to a value favorable to that edge. An active 1-edge drops out of the the set of active edges at the first point in time when three of its vertices are colored 1. Likewise, an active 0-edge drops out of the the set of active edges at the first point in time when two of its vertices are colored 0.

It remains to show that eventually, the set of active edges becomes empty. To show this, we show that as long as some active edge exists, the algorithm can make progress (color some vertices and drop an active edge). Consider an arbitrary intermediate step of the algorithm, with the set of active 1-edges remaining being $C_A$ and the set of active 0-edges remaining being $B_A$. Some vertices belong both to edges in $B_A$ and to edges in $C_A$. These vertices are uncolored at this point. Every other vertex is either previously colored, or may be colored at this point: if it only belongs to $C_A$ it is colored 1, if it only belongs to $B_A$ it is colored 0. We show that after completing this coloring operation, necessarily at least one active edge becomes legally colored and can drop from the active set.

Let $m'$ denote the number of vertices in $B_A \cup C_A$. If no edge from $B_A$ has two colored vertices then $m' \leq 4|C_A| + |B_A|$. If no edge from $C_A$ has three colored vertices, then $m' \leq 2|C_A| + 4|B_A|$. Adding twice the first inequality with three times the second inequality we obtain that $5m' \leq 14|B_A \cup C_A|$. This contradicts the expansion property. Hence some active edge must have sufficiently many colored vertices, and it can drop out of the active set.

In summary, the trivial algorithm that only colors vertices that are not under contention and drops legally colored edges, necessarily produces a legal $(3, 2)$-coloring whenever $\alpha > 14/5$.

A value of $\alpha > 14/5$ is necessary for the trivial algorithm. For example, when $|C_A| = 3$ and $|B_A| = 2$, there may be 6 vertices belonging only to $C_A$ (and colored 1), 2 vertices belonging to $B_A$ (and colored 0), and 6 shared vertices, for a total of 14 vertices. The trivial algorithm cannot make any progress at this point. We now wish to show that a value of $\alpha = 8/3$ also suffices. For this, we shall use a more sophisticated coloring algorithm.

**Definition 4.3** *For a set $E$ of edges, a* preliminary coloring *is defined as follows. Consider the subhypergraph induced on $E$ (dropping all other hyperedges and vertices). Color vertices that appear only in 0-edges by 0, and set the* demand *of every 0-edge in $E$ to be $q$ minus the number of vertices in that 0-edge already colored 0. Color vertices that appear only in 1-edges by 1, and set the demands of the 1-edges in $E$ to $p$ minus the number of vertices in that 1-edge already colored 1. The set $E$ is* admissible *if none of its edges is legally colored by this process. A hypergraph satisfies the* counting condition *if for every choice of admissible $E$, following the respective preliminary coloring, the number of remaining (uncolored) vertices is at least as large as the sum of demands of the edges.*

**Lemma 4.4** *Every 4-uniform hypergraph with expansion $\alpha \geq 8/3$ satisfies the counting condition.*

**Proof**: Consider an arbitrary admissible set $E$ of hyperedges and perform the preliminary coloring. Let $C_i$ (for $i = 0, 1, 2$) denote the number of 1-edges with $i$ precolored vertices, and let $B_i$ (for $i = 0, 1$) denote the number of 0-edges with $i$ precolored vertices. Let $m$ denote the total number of vertices spanned by $E$, and let $m_2$ denote the number of vertices that are members of both 0-edges and 1-edges in $E$. Then we have that $m_2 \leq 4B_0 + 3B_1$ (because every vertex counted in $m_2$ must belong to some 0-edge and not be precolored). Assume now for the sake of contradiction that the counting condition does not hold. Then $m_2 < 3C_0 + 2C_1 + C_2 + 2B_0 + B_1$. Adding twice this last inequality to the former inequality and dividing by three we get $m_2 < 2C_0 + \frac{4}{3}C_1 + \frac{2}{3}C_2 + \frac{8}{3}B_0 + \frac{5}{3}B_1$. Now

$$m \leq C_1 + 2C_2 + B_1 + m_2 < 2C_0 + \frac{7}{3}C_1 + \frac{8}{3}C_2 + \frac{8}{3}B_0 + \frac{8}{3}B_1 \leq \frac{8}{3}|E|$$

which contradicts the expansion property. □

The value of $\alpha = 8/3$ in the lemma is best possible, as can be seen by the example following the statement of Theorem 4.3. Note also that if $E$ is not required to be admissible, no expansion below $\alpha = 3$ suffices in order to obtain the counting condition. Consider the following example with $k + 2(k + 1) + 3k$ vertices. There are $k + 1$ 1-edges, each having two unshared vertices (contributing the term $2(k+1)$), and $k$ 0-edges each having three unshared vertices (contributing the term $3k$). The other vertices in the above hyperedges are taken from a pool of $k$ shared

vertices. The 0-edges can be legally colored by their unshared vertices, and hence $E$ is not admissible. The 1-edges have a demand of $k+1$ on the $k$ shared vertices, so the counting condition does not hold. (This of course does not mean that the demand cannot be met.)

**Lemma 4.5** *Every hypergraph satisfying the counting condition is $(p,q)$-colorable.*

**Proof**: Perform the trivial greedy algorithm until no progress can be made. At this point, the counting condition implies that the number of uncolored vertices is at least as large as the demand of the remaining edges. If this is true also for every subset of remaining edges and their vertices, then Hall's theorem implies that vertices can be matched to edges such that every edge has at least as many vertices as its demand. Every edge can color the vertices matched to it by its preferred color, meeting all demands and obtaining a $(p,q)$-coloring. Hence it remains to consider the case that some set of edges contains fewer vertices than the sum of the demands of its members. Consider a maximal set $E'$ of such edges, and let $E$" be the remaining edges not in $E'$. Observe that the counting condition implies that $E$" is nonempty. Moreover, using only vertices not in $E'$, the set $E$" and the remaining vertices satisfy Hall's condition with respect to the demand of $E$" (otherwise $E'$ is not maximal). It follows that the demand of $E$" can be satisfied without coloring any of the uncolored vertices in $E'$. Thereafter, the counting condition is violated, implying that at least one of the uncolored vertices (in $E'$) is demanded either only by 1-edges or only by 0-edges. Hence the trivial greedy algorithm can be resumed and make progress.

Alternating as above between the trivial greedy algorithm and a matching algorithm, at no point in time is there an unsatisfied edge with a vertex colored differently than its demand, and progress can be made as long as there are uncolored vertices. Hence eventually, one obtains a legal $(p,q)$-coloring. □

The combination of Lemmas 4.4 and 4.5 completes the proof of Theorem 4.3. The proof of Theorem 4.3 is algorithmic, because the algorithm in the proof of Lemma 4.5 can be run in polynomial time, using flow techniques (details omitted). We can now prove Lemma 4.1.

**Proof**: We start by applying the trivial algorithm. We claim that at the point when the trivial algorithm cannot make any progress, at most $n$ active 0-edges remain. Let $B_A$ be the set of active 0-edges that remain, and let $C_A$ be the set of active 1-edges that remain, and assume for the sake of contradiction that $|B_A| > n$. Consider an arbitrary subset $B'_A \subset B_A$ with $|B'_A| = n$. Observe that $C_A$ contains at most $4|C_A|$ distinct vertices. No edge in $B'_A$ has two vertices (or more) not in $C_A$, because otherwise it cannot be active. Hence the total number of vertices in $B'_A \cup C_A$ is at most $4|C_A| + n \leq \frac{5}{2}|B'_A \cup C_A|$ (the last inequality follows because $C_A \leq n$). This contradicts the expansion conditions of the corollary (observe that $|B'_A \cup C_A| \leq 2n$).

Once the set of active 0-edges drops to $n$, the total number of active edges is at most $2n$, and the partial coloring has the property that for every active edge, none of its vertices is colored to a color different than the edge's demand. At this point Theorem 4.3 applies, and the $(3,2)$-coloring can be completed. The whole coloring algorithm runs in polynomial time, by the discussion preceding this proof. □

A straightforward modification to the proof of Lemma 4.1 shows that if all sets of at most $3n$ hyperedges have expansion $8/3$, then a legal $(3,2)$-coloring exists also if the chosen $n$ edges are 0-edges and the remaining edges are 1-edges.

# 5 Open problems

- The proofs of Theorems 1.1 and 1.2 are by explicit constructions of the corresponding schemes, but those of Theorems 1.4 and 1.5 rely on the existence of strong expanders proved by probabilistic arguments. The known constructions of explicit lossless expanders (see [8]) can provide some explicit versions of these schemes, but the number of probes will increase significantly (though will stay constant for the appropriate range of parameters $n, m$ and $s$.)

- There are still rather substantial gaps between the upper and lower bounds for the minimum required space in most cases considered here; it will be nice to get tighter estimates. It particular, it will be interesting to decide if there are adaptive $(n, m, s, 2)$-schemes with $s < m$ for $n > \sqrt{m}/2$, and to identify the behavior of the largest $n = n(m)$ so that there are adaptive $(n, m, s, 2)$-schemes with $s = o(m)$.

### Acknowledgements

We thank Bill Gasarch and Matt McCutchen for their useful comments on an earlier version of this manuscript.

# References

[1] N. Alon and A. Shapira, On an extremal hypergraph problem of Brown, Erdős and Sós, Combinatorica 26 (2006), 627-645.

[2] B. Bloom, Space/time tradeoffs in hash coding with allowable errors, Communications of the ACM 13:7 (1970), 422–426.

[3] B. Bollobás, **Random Graphs**, Academic Press, 1985.

[4] A. Broder and M. Mitzenmacher, Network applications of Bloom filters: a survey, Internet Mathematics Vol. 1, No. 4: 485–509, 2004.

[5] W. G. Brown, P. Erdős and V.T. Sós, Some extremal problems on $r$-graphs, New Directions in the Theory of Graphs, Proc. $3^{rd}$ Ann Arbor Conference on Graph Theory, Academic Press, New York, 1973, 55-63.

[6] W. G. Brown, P. Erdős and V.T. Sós, On the existence of triangulated spheres in 3-graphs and related problems, Periodica Mathematica Hungaria, 3 (1973), 221-228.

[7] H. Buhrman, P. B. Miltersen, J. Radhakrishnan and S. Venkatesh, Are bitvectors optimal?, Proc. STOC 2000, 449-458. Also: SIAM J. Computing 31 (2002), 1723-1744.

[8] M. Capalbo, O. Reingold, S. Vadhan and A. Wigderson, Randomness conductors and constant-degree lossless expanders, Proc. STOC 2002, 659-668.

[9] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, A new series of dense graphs of high girth, Bull. Amer. Math. Soc. (N.S.), 32 (1995), 73-79.

[10] M. Minsky and S. Papert, *Perceptrons*, MIT Press, Cambridge, MA 1969.

[11] J. Radhakrishnan, V. Raman and S. S. Rao, Explicit deterministic constructions for membership in the bitprobe model, Proc. ESA 2001, Lecture Notes in Computer Science, Vol. 2161 (2001), 290–299.

[12] I. Z. Ruzsa and E. Szemerédi, Triple systems with no six points carrying three triangles, in Combinatorics (Keszthely, 1976), Coll. Math. Soc. J. Bolyai 18, Volume II, 939-945.

[13] G. N. Sárközy and S. M. Selkow, On a Turán-type hypergraph problem of Brown, Erdős and T. Sós, Discrete Math. 297 (2005), 190–195