MINIMUM AVERAGE DISTANCE SUBSETS IN THE HAMMING CUBE

André Kündgen

August 12, 1999

Abstract. In 1977, Ahlswede and Katona proposed the following isoperimetric problem: find a set S of n points in $\{0,1\}^k$ whose average Hamming distance is minimal – or equivalently find an n-vertex subgraph of the hypercube Q_k whose average distance is minimal.

We report on some recent results and conjecture that S can be chosen to be the set of all points in $\{0,1\}^k$ that are distance at most r from some point $c \in \mathbb{R}^k$. We show that these "discrete balls" include all known good constructions and we provide additional evidence supporting the conjecture.

1. Discrete isoperimetric problems

The classic isoperimetric problem consists of showing that in Euclidean space $\mathbb{R}^k$ (originally only for $k = 2$), the (convex) body with smallest surface area, given a fixed volume, is the sphere. See Santaló [S] for a comprehensive book on related geometric questions.

The discrete isoperimetric problem (solved by Harper [H] and Katona [Ka1]) asks the corresponding question for the Hamming space $\{0,1\}^k$: find a set of n points, so that the boundary is minimal. Not surprisingly the answer is the Hamming sphere. For a short proof see Frankl and Füredi [FF]. The survey of Bezrukov [Bz] discusses various discrete isoperimetric problems.

In 1918, Blaschke [Bl] solved another isoperimetric problem in $\mathbb{R}^2$ by showing that the convex body of smallest mean distance, given a fixed volume, is the disk. In 1977, Ahlswede and Katona [AK] proposed the discrete analog of Blaschke's problem: find a set S of n points in Hamming space $\{0,1\}^k$ whose average Hamming distance is minimal. Or equivalently, find an n-vertex subgraph of the hypercube Q_k with minimal average distance. This problem has been recently investigated by several authors [AA, AS, F, FWY, XF]. Up to a constant factor the Hamming sphere achieves the minimum, but it is not necessarily best possible. It is the aim of this paper to suggest an analog of the sphere for the discrete case: the *discrete ball*. We conjecture that the optimum is always achieved by a discrete ball and we provide some supporting evidence.

1991 *Mathematics Subject Classification.* 05D05, 05C12, 90C05.

Key words and phrases. discrete isoperimetric problem, minimum average distance, discrete ball, hamming distance, hypercube.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

2. Definitions and known results

Definition 1. The *Hamming distance* between two points $x, y \in \{0,1\}^k$, denoted by $d(x,y)$, is the number of coordinates in which they differ,

$$d(x,y) := \sum_{1 \leq i \leq k} |x_i - y_i|.$$

The *weight* of a point $x \in \{0,1\}^k$ is its number of non-zero entries, $w(x) := d(0,x)$, where 0 is the zero vector. The *distance-sum* of a set $S \subset \{0,1\}^k$ is given as

$$d(S) := \sum \{d(x,y) : \{x,y\} \in \binom{S}{2}\}.$$

The *weight of a coordinate* i of a set S is the number of ones in that coordinate among the points in S

$$w_i(S) := \sum_{x \in S} x_i.$$

A fundamental observation is that

$$d(S) = \sum_{i=1}^{k} w_i(S)(|S| - w_i(S)). \tag{1}$$

Indeed, both sums count the number of triples (x, y, i) with $x_i = 1$ and $y_i = 0$.

The problem of Ahlswede and Katona [AK] amounts to determining, for all $2 \leq n \leq 2^k$,

$$f(n,k) := \min\{d(S) : S \subset \{0,1\}^k, |S| = n\}.$$

Any set S achieving $f(n,k)$ will be called *extremal*. In general, the structure of extremal sets seems elusive since there are two different configurations that are optimal in a number of cases: the (Hamming) sphere and the (sub)cube. We will define both notions for general n.

Definition 2. The *Hamming sphere* of radius $r \geq 0$ centered at $x \in \{0,1\}^k$ is defined as

$$B(x,r) = \{y \in \{0,1\}^k : d(x,y) \leq r\}.$$

Every set $S \subset \{0,1\}^k$, for which there is a t such that $B(0, t-1) \subset S \subset B(0,t)$ will be called a *(generalized Hamming) sphere*. The generalized Hamming sphere in which we pick the lexicographically smallest vectors for weight t will be denoted by $B_k(n)$.

The set consisting of the n lexicographically smallest vectors in $\{0,1\}^k$ is the *subcube* $Q_k(n)$. We frequently drop the subscripts in $B_k(n)$ and $Q_k(n)$.

For example $Q_5(5) = \{00000, 00001, 00010, 00011, 00100\}$ is not a sphere since it contains a vector of weight 2, but misses some vectors of weight 1. It can be seen that $B_k(n) = Q_k(n)$ if and only if $n \leq 3$ or $n \geq 2^k - 3$. Note that if we denote the binary expansion of m by $b(m)$, that is $m = \sum_{i=1}^k b(m)_i 2^{k-i}$, then $Q(n) = \{b(0), b(1), \ldots, b(n-1)\}$.

Although there seem to be no closed formulas for $d(B_k(n))$ or $d(Q(n))$, $d(Q(n))$ can be computed efficiently with the following recurrence relation.

Proposition 1. *$d(Q(n)) = \lfloor n^2/4 \rfloor + 2d(Q(\lfloor n/2 \rfloor)) + 2d(Q(\lceil n/2 \rceil))$, so that*

$$d(Q(n)) = \frac{1}{4} n^2 \lg n + \mathrm{O}(n^2),$$

where lg *denotes the base 2 logarithm.*

Proof. If we abbreviate $w_i(Q(n)) = q(n)$, then

$$\begin{aligned}
&[q(\lfloor n/2 \rfloor) + q(\lceil n/2 \rceil)][n - q(\lfloor n/2 \rfloor) - q(\lceil n/2 \rceil)] \\
&\qquad = q(\lfloor n/2 \rfloor)[\lfloor n/2 \rfloor - q(\lfloor n/2 \rfloor)] + q(\lfloor n/2 \rfloor)[\lceil n/2 \rceil - q(\lceil n/2 \rceil)] \\
&\qquad + q(\lceil n/2 \rceil)[\lfloor n/2 \rfloor - q(\lfloor n/2 \rfloor)] + q(\lceil n/2 \rceil)[\lceil n/2 \rceil - q(\lceil n/2 \rceil)] \\
&\qquad = 2q(\lfloor n/2 \rfloor)[\lfloor n/2 \rfloor - q(\lfloor n/2 \rfloor)] + 2q(\lceil n/2 \rceil)[\lceil n/2 \rceil - q(\lceil n/2 \rceil)].
\end{aligned}$$

The last equality clearly holds if $q(\lceil n/2 \rceil) = q(\lfloor n/2 \rfloor)$. Otherwise we observe that we must have $q(\lceil n/2 \rceil) = q(\lfloor n/2 \rfloor) + 1$ and $\lceil n/2 \rceil = \lfloor n/2 \rfloor + 1$, so that the equation also follows easily. Furthermore, note that

$$\begin{aligned}
&\{x \in \{0,1\}^{k-1} : (x_1, x_2, \ldots, x_{k-1}, 1) \in Q_k(n)\} = Q_{k-1}(\lfloor n/2 \rfloor), \text{ and} \\
&\{x \in \{0,1\}^{k-1} : (x_1, x_2, \ldots, x_{k-1}, 0) \in Q_k(n)\} = Q_{k-1}(\lceil n/2 \rceil),
\end{aligned}$$

so that

$$\begin{aligned}
d(Q(n)) - \lfloor n^2/4 \rfloor &= \sum_{i=1}^{k} w_i(Q_k(n))[n - w_i(Q_k(n))] - \lfloor n^2/4 \rfloor \\
&= \sum_{i=1}^{k-1} [w_i(Q_{k-1}(\lfloor n/2 \rfloor)) + w_i(Q_{k-1}(\lceil n/2 \rceil))] \times \\
&\qquad \times [n - w_i(Q_{k-1}(\lfloor n/2 \rfloor)) - w_i(Q_{k-1}(\lceil n/2 \rceil))] \\
&= 2\sum_{i=1}^{k-1} q(\lfloor n/2 \rfloor)[\lfloor n/2 \rfloor - q(\lfloor n/2 \rfloor)] + 2\sum_{i=1}^{k-1} q(\lceil n/2 \rceil)[\lceil n/2 \rceil - q(\lceil n/2 \rceil)] \\
&= 2d(Q(\lfloor n/2 \rfloor)) + 2d(Q(\lceil n/2 \rceil)).
\end{aligned}$$

For the asymptotics observe that $d(Q(n)) \leq \lfloor n^2/4 \rfloor \lceil \lg n \rceil$ is immediate since at most $\lceil \lg n \rceil$ of the $w_i(Q(n))$ are nonzero. So it suffices to prove that for $n \geq 1$,

$d(Q(n)) \geq (n^2/4)\lg n$. This is true for $n \leq 3$, so that we can proceed by induction on n. If $n \geq 4$ is even, then

$$d(Q(n)) = \frac{n^2}{4} + 4d(Q(n/2)) \geq \frac{n^2}{4} + (n/2)^2 \lg(n/2) = \frac{n^2}{4}\lg n.$$

If $x > 0$ and $x + c > 0$ then $\lg(x+c) \geq \lg x + \frac{c}{(x+c)\ln 2}$, so that for odd $n \geq 5$,

$$\begin{aligned}
d(Q(n)) &= \frac{n^2-1}{4} + 2d(Q((n-1)/2)) + 2d(Q((n+1)/2)) \\
&\geq \frac{n^2-1}{4} + \frac{(n-1)^2}{8}\lg((n-1)/2) + \frac{(n+1)^2}{8}\lg((n+1)/2) \\
&= -\frac{1}{2} + \frac{(n-1)^2}{8}\lg(n-1) + \frac{(n+1)^2}{8}\lg(n+1) \\
&= -\frac{1}{2} + \frac{n^2+1}{8}\lg(n^2-1) + \frac{n}{4}(\lg(n+1) - \lg(n-1)) \\
&\geq -\frac{1}{2} + \frac{n^2+1}{8}\left(\lg n^2 - \frac{1}{(n^2-1)\ln 2}\right) + \frac{n}{4}\left(\frac{2}{(n+1)\ln 2}\right) \\
&= \frac{n^2}{4}\lg n + \frac{\lg n}{4} - \frac{1}{2} + \frac{4n(n-1) - (n^2+1)}{8(n^2-1)\ln 2} \geq \frac{n^2}{4}\lg n. \quad \square
\end{aligned}$$

It is left as an exercise that for any Hamming sphere S, with $|S| = n$

$$\frac{n}{2}\, w(S) \leq f(n,k) \leq d(S) \leq n\, w(S), \tag{2}$$

where $w(S) = \sum_{i=1}^{k} w_i(S)$ is a lower bound on the distance sum from a fixed point x, $\sum_{y \in S} d(x,y)$. Hence the Hamming spheres are optimal up to a factor of 2. However, deciding which Hamming sphere has the smallest distance sum seems as hard a problem as determining $f(n,k)$. In general, $B_k(n)$ has a small distance sum, but for example if $k + 5 \leq n \leq 2k$ then picking the $n - (k+1)$ vectors of weight 2 so that they all have a 1 in a fixed position is uniquely optimal.

Definition 3. For $x \in \{0,1\}^k$ we let $r_i(x) = (x_1, \ldots, x_{i-1}, 1 - x_i, x_{i+1}, \ldots, x_k)$ and say that $r_i(S) = \{r_i(x) : x \in S\}$ is a *zero-one swap* in coordinate i. Let $r(x) := r_1(r_2(\ldots(r_k(x))\ldots))$ denote the unique vector with $d(x, r(x)) = k$. For example $\vec{\jmath} = r(0)$ is the all ones vector. We define $r(S) := r_1(r_2(\ldots(r_k(S))\ldots))$ similarly.

Furthermore, let $s_{ij}(x) = y$ be the vector with $y_i = x_j$, $y_j = x_i$ and $y_\ell = x_\ell$ for $\ell \neq i, j$. The corresponding $s_{ij}(S)$ is a *coordinate swap.*

We say that two subsets of $\{0,1\}^k$ are *isomorphic* if one can be obtained from the other by a sequence of coordinate swaps and zero-one swaps. By (1) isomorphic sets have the same distance-sum.

The first exact values, and extremal configurations, were found by Jaeger, Khelladi and Mollard:

Theorem 1 [JKM]. *$f(4,k) = d(Q(4)) = 8$, $f(8,k) = d(Q(8)) = 48$, whereas $f(n,k) = (n-1)^2$ is achieved by a sphere for $k \geq n-1$, $n \neq 4, 8$. The extremal sets are unique, up to isomorphism, unless $5 \leq n \leq 7$, when both $Q_k(n)$ and $B_k(n)$ are extremal.*

Jaeger, Khelladi and Mollard where actually interested in a matroid theoretical question suggested by Tarsi [T], who already stated the values for $n \leq 8$ in Theorem 1 without proof. Jamshy and Tarsi [JT] established the cases $n \geq 9$ by a short inductive argument (omitting the base case), and stated that Alon also obtained Theorem 1 independently. Another independent proof of Theorem 1 can be found in Kündgen [K].

Next, Althöfer and Sillke proved the following isoperimetric inequality

Theorem 2 [AS]. *If $S \subset \{0,1\}^k$ and $|S| = n$, then*

$$d(S) \geq \frac{n}{4}(n(k+1) - 2^k),$$

with equality only for $S \simeq Q(2^{k-1}), Q(2^k)$.

This yields $f(2^{k-1}, k)$ and again a subcube is the unique optimal configuration. Fu [F] found a different proof of Theorem 2 that yields a slightly better inequality. Xia and Fu improved Theorem 2 in the case that n is odd and very recently Fu, Wei and Yeung improved the bounds even further. Altogether, their theorems imply

Theorem 3 [XF,FWY]. *The subcube is extremal if $n = 2^{k-1} \pm 1$, $2^{k-1} \pm 2$, 2^{k-2} or $2^{k-2} \pm 1$.*

Notice that the previous bounds are only useful when n is at least of size about $2^k/k$. For the case when n grows rather like c^k for some $1 < c < 2$, Ahlswede and Althöfer determined $f(n,k)$ asymptotically

Theorem 4 [AA]. *For any constant $0 < a < 1/2$,*

$$\binom{k}{\lfloor ak \rfloor}^{-2} f(\binom{k}{\lfloor ak \rfloor}, k) = ka(1-a) - \mathrm{o}(k).$$

Theorem 4 is asymptotically achieved by taking all $x \in \{0,1\}^k$ with weight $w(x) = \lfloor ak \rfloor$. Although this suggests that in this range of n suitable Hamming spheres are extremal, this is far from certain.

2. Structure of extremal configurations

Definition 4. A set $S \subset \{0,1\}^k$ is a *down-set* (respectively *up-set*) if $x \in S$ with $x_i = 1$ ($x_i = 0$) implies that $r_i(x) \in S$. Down-sets are also called *ideals*.

We say S is *right-shifted* (respectively *left-shifted*) if $x \in S$ with $x_i = 1$ and $x_j = 0$ for some $i < j$ ($i > j$) implies $s_{ij}(x) \in S$.

If $w_1(S) \leq w_2(S) \leq \cdots \leq w_k(S) \leq |S|/2$, then S is in *standard form*.

If S is a down-set, then $w_i(S) \leq |S|/2$ and if S is right-shifted, then $w_i(S) \leq w_{i+1}(S)$, and thus every right-shifted down-set is in standard form. We will first reduce our problem to right-shifted down-sets.

Proposition 2. *Let $S \subset \{0,1\}^k$ be an extremal set.*

a) S is in standard form if and only if S is a right-shifted down-set.

b) S is isomorphic to a unique S' in standard form.

c) If S is in standard form with $0 \leq a_1 < a_2 < \cdots < a_\ell = |S|/2$, so that for k_j coordinates $w_i(S) = a_j$ and $\sum k_j = k$, then there are exactly

$$\frac{k!\, 2^{k-k_\ell}}{k_1!\, k_2! \cdots k_\ell!}$$

extremal sets isomorphic to S.

Proof. Suppose that S is an extremal set in standard form. S must be a down-set, since otherwise there is $x \in S$ and $y \notin S$ with $x_j = 1$, $y_j = 0$ and $x_i = y_i$, for $i \neq j$. But (1) implies that

$$d(S) - d(S - x + y) = |S| - 2w_j(S) + 1 > 0.$$

Similarly if S is not right-shifted, there is $x \in S$ and $y \notin S$ with $x_j = y_\ell = 1$, $x_\ell = y_j = 0$, (for $j < \ell$) and $x_i = y_i$, for $i \neq j, \ell$. Again

$$d(S) - d(S - x + y) = 2(w_\ell(S) - w_j(S) + 1) > 0$$

contradicting the extremality of S and finishing the proof of a).

b) Using zero-one swaps in coordinates of weight greater than $|S|/2$ and then arranging the coordinates in an increasing fashion we see that S is isomorphic to some S'. To see that S' is unique it suffices to see that swapping coordinates of equal weight and zero-one swapping coordinates of weight $|S|/2$ doesn't change S'. Indeed suppose that $x \in S'$ and $w_i(S') = w_j(S')$ with $i < j$. Now $s_{ij}(x) = x$, unless exactly one of x_i, x_j is zero. However, if $x_i = 1$ and $x_j = 0$, then $x \in S'$ since S' is right-shifted, and the same holds if $x_i = 0$ and $x_j = 1$, since otherwise $w_i(S') < w_j(S')$. If $x \in S'$, then changing x_k from one to zero results in a vector in S', since S' is a down-set, and changing a zero to a one does also, unless $w_k(S') < |S'|/2$. Part c) is now obvious. □

So from now on we can assume that optimal sets are in standard form. Next we investigate complements of extremal sets.

Proposition 3. *Let $S \subset \{0,1\}^k$ and $\overline{S} = \{0,1\}^k \setminus S$.*

a) $d(\overline{S}) = d(S) + k2^{k-1}(2^{k-1} - |S|)$.

b) $f(k, 2^k - n) = f(k,n) + k2^{k-1}(2^{k-1} - n)$.

c) The complement of an extremal set for $f(n,k)$ is extremal for $f(2^k - n, k)$.

d) If S is a down-set (up-set, right-shifted, left-shifted) then $\overline{S}$ and $r(S)$ are up-sets (down-sets, left-shifted, right-shifted).

e) If S is a standard extremal set, then $r(\overline{S}) = \overline{r(S)}$ is a standard extremal set.

Proof. a) Let $|S| = n$. Then

$$\begin{aligned} d(\overline{S}) &= \sum_{i=1}^{k} w_i(\overline{S})(2^k - n - w_i(\overline{S})) = \sum_{i=1}^{k}(2^{k-1} - w_i(S))(2^{k-1} - n + w_i(S)) \\ &= \sum_{i=1}^{k} \left(w_i(S)(n - w_i(S)) + 2^{2k-2} - n2^{k-1}\right) = k2^{k-1}(2^{k-1} - n) + d(S). \end{aligned}$$

Now b) and c) follow immediately, since $d(\overline{S})$ is minimal exactly when $d(S)$ is. Finally d) follows from the definitions and implies e). □

So from now on, since there is a correspondence between sets and their complement (and since the central case $n = 2^k/2$ has been solved), we may assume that $n < 2^{k-1}$.

We also observe that the cubes and spheres (if we pick the "right" points of weight t) meet the basic requirements for extremal sets in standard form: they are right-shifted down-sets. Also, the complement of a sphere is a sphere centered at $111\dots1$ and thus isomorphic to a sphere, for example $\overline{B_k(n)} = r(B_k(2^k - n))$, and

$$\begin{aligned} \overline{Q(n)} &= \{b(n), b(n+1), \dots, b(2^k - 1)\} \\ &= r(\{b(2^k - 1 - n), b(2^k - 1 - (n+1)), \dots, b(0)\}) \\ &= r(Q(2^k - n)) \simeq Q(2^k - n). \end{aligned}$$

3. Discrete balls

We will now give the main definition,

Definition 5. For $x, y \in \mathbb{R}^k$ let $d_p(x, y) := \|x - y\|_p$ be their *L_p-distance*, where for $1 \le p < \infty$ the L_p-norm is defined by

$$\|x\|_p := \left(\sum_{i=1}^{k} |x_i|^p\right)^{1/p}.$$

For $c \in \mathbb{R}^k$, $r \ge 0$ and $1 \le p$ we can define the *discrete L_p-ball*

$$B_p(c, r) := \{x \in \{0,1\}^k : d_p(c, x) \le r\}.$$

Also for $y \in \mathbb{R}$ let $f_p(y) := |1 - y|^p - |y|^p$; for example $f_2(y) = 1 - 2y$.

The L_p-distance is a natural extension of the Hamming distance, so that every Hamming sphere is a discrete L_p-ball, $B(x, r) = B_p(x, r^{1/p})$ (for $x \in \{0,1\}^k$ and $r \ge 0$). It is easy to see that all discrete L_∞-balls, where $\|x\|_\infty := \max\{|x_i| : 1 \le i \le k\}$, are isomorphic to subcubes $Q(2^i)$ for some i. This is not interesting for us, so throughout we will assume that $1 \le p < \infty$.

The following simple observation is essential in our study of the properties of discrete balls.

Observation. If $c \in \mathbb{R}^k$ and $x \in \{0,1\}^k$, then

$$d_p(c,x)^p = \|c\|_p{}^p + \sum_{x_i=1} f_p(c_i). \tag{3}$$

The following theorem will show, perhaps somewhat surprisingly, that the collection of L_p-balls is independent of p.

Theorem 5. *For all $c \in \mathbb{R}^k$, $r \geq 0$, such that $B_p(c,r) \neq \emptyset$*
a) $B_p(c,r) = B_2(\overline{c}, \overline{r})$, where $\overline{c}_i = \frac{1}{2}(1 - f_p(c_i))$ and $\overline{r} = \sqrt{r^p - \|c\|_p^p + \|\overline{c}\|_2^2}$.
b) If $c \in [0,1]^k$, then $B_2(c,r) = B_1(c,\overline{r})$, where $\overline{r} = r^2 - \|c\|_2^2 + \|c\|_1$.
c) $B_2(c,r) = B_2(\overline{c},\overline{r})$ for some $\overline{c} \in [0,1]^k$, $\overline{r} \in \mathbb{R}$.

Proof. a) follows from the observation that for any $x \in \{0,1\}^k$,

$$d_p(c,x)^p - \|c\|_p^p = \sum_{x_i=1} f_p(c_i) = \sum_{x_i=1} f_2((1 - f_p(c_i))/2) = d_2(\overline{c},x)^2 - \|\overline{c}\|_2^2.$$

For b) note that if $0 \leq y \leq 1$, then $f_1(y) = f_2(y)$, so that we conclude similarly that $d_2(c,x)^2 - \|c\|_2^2 = d_1(c,x) - \|c\|_1$.

For c), fix $m > 0$, and set $c'_i = \frac{1}{2m}(m - 1 + 2c_i)$ and

$$r' = \frac{1}{m}\sqrt{mr^2 - m\|c\|_2^2 + m^2\|c'\|_2^2}.$$

We will show that $B_2(c,r) = B_2(c',r')$. From this the result will follow by choosing m sufficiently large – note that as an additional bonus we can choose $\overline{c}$ as close to $(1/2,\ldots,1/2)$ as we wish. Indeed,

$$\begin{aligned} d_2(c,x)^2 - \|c\|_2^2 &= \sum_{x_i=1} f_2(c_i) = \sum_{x_i=1} (1 - 2c_i) = \sum_{x_i=1} m(1 - 2c'_i) \\ &= m \sum_{x_i=1} f_2(c'_i) = m(d_2(c,x)^2 - \|c'\|_2^2). \quad \square \end{aligned}$$

Remarks. By observing that f_q is invertible when $1 < q$, we could have replaced B_2 in a) by B_q which would have shown that all p are equivalent. Even so, we know that we don't lose any generality by restricting our attention to $p = 1, 2$. So from now on we will simply refer to *discrete balls*, and only specify p if necessary. Furthermore we can assume that $c \in [0,1]^k$.

We will now investigate the properties of discrete balls. Let q be the vector with $q_i = 2^{-i}$.

Proposition 4.

a) The isomorphic image of a discrete ball is a discrete ball

b) For a discrete ball $B = B_2(c, r)$ the following are equivalent:

i) *B is a right-shifted down-set,*

ii) *B is in standard form, and*

iii) *we can assume that $(0 \leq)c_1 \leq c_2 \leq \cdots \leq c_k \leq 1/2$.*

c) $\overline{B_2(c, r)} = B_2(\overline{c}, \overline{r})$, where $\overline{c} = \vec{\jmath} - c$ and $\overline{r}^2 = \|c\|_2^2 + \|\overline{c}\|_2^2 - r^2 - \varepsilon$ for some $\varepsilon > 0$.

d) For $0 \leq m \leq 1$ and $0 \leq \varepsilon \leq 2m$

$$d_1(m\vec{\jmath} - \varepsilon q, b(n)) = mk - \varepsilon(1 - 2^{-k}) + (1 - 2m)w(b(n)) + \varepsilon n 2^{1-k}.$$

e) $Q(n) = B_1(c, r)$, with $c = \frac{1}{2}\vec{\jmath} - q$ and $r = d_1(c, b(n-1))$.

f) $B(n) = B_1(c, r)$, with $c = \frac{1}{4}\vec{\jmath} - \frac{1}{2}q$ and $r = d_1(c, y)$ for y the lexicographically biggest vector of weight t in $B(n)$.

Proof. a) Since $d_p(c, x) = d_p(r_i(c), r_i(x))$ it follows that $r_i(B_p(c, r)) = B_p(r_i(c), r)$ and $s_{ij}(B_p(c, r)) = B_p(s_{ij}(c), r)$.

For b), i) implies ii) is immediate. To see that iii) implies i), assume that $c_1 \leq \cdots \leq c_k \leq 1/2$. Since $c_i \leq 1/2$ and $x_i = 1$ implies that $d_2(c, x) \geq d_2(c, r_i(x))$, B is a down-set. Similarly, if for $i < j$, $x_i = 1$ and $x_j = 0$, then

$$d_2(c, x)^2 - d_2(c, s_{ij}(x))^2 = f_2(c_i) - f_2(c_j) = 2(c_j - c_i) \geq 0,$$

so that B is right-shifted. For ii) implies iii) suppose that $w_1(B) \leq w_2(B) \leq \cdots \leq w_k(B) \leq |B|/2$. By Theorem 5 we can assume that $c \in [0, 1]^k$ and $B = B_1(c, \overline{r})$. Suppose $c_i \geq 1/2$. Then $x \in B$ with $x_i = 0$ implies $r_i(x) \in B$, so that $w_i(B) \geq |B|/2 \geq w_i(B)$. So equality must hold and therefore $x \in B$ exactly when $r_i(x) \in B$. We see that $B = B_1(c', \overline{r})$ where $c'_i = 1/2$ and $c'_j = c_j$ for $j \neq i$. Indeed, if $x \in B$, $x_i = 0$, then

$$\overline{r} \geq d_1(c, x) \geq d_1(c', x) = d_1(c', r_i(x)),$$

and if $x \notin B$, $x_i = 1$, then

$$\overline{r} < d_1(c, x) \leq d_1(c', x) = d_1(c', r_i(x)).$$

Furthermore, if $c_i \geq c_j$ for $i < j$, then $x \in B$ with $x_i = 0$ and $x_j = 1$ implies that $s_{ij}(x) \in B$, so that $w_i(B) \geq w_j(B) \geq w_i(B)$. Again we conclude that $x \in B$ exactly when $s_{ij}(x) \in B$. So $B = B_1(c', \overline{r})$ where $c'_i = c'_j = (c_i + c_j)/2$ and $c'_\ell = c_\ell$ for $\ell \neq i, j$. Indeed, $\|c\|_1 = \|c'\|_1$ and

$$f_1(c_i) + f_1(c_j) = 2(1 - c_i - c_j) = f(c'_i) + f(c'_j),$$

so that $d_1(c, x) = d_1(c', x)$ unless $x_i \neq x_j$. Finally, if $x \in B$, $x_i = 0$, $x_j = 1$, then

$$\overline{r} \geq d_1(c, x) \geq d_1(c', x) = d_1(c', s_{ij}(x)),$$

and if $x \notin B$, $x_i = 1$, $x_j = 0$, then

$$\overline{r} < d_1(c,x) \le d_1(c',x) = d_1(c', s_{ij}(x)).$$

This finishes the proof of b). For the proof of c) pick $\varepsilon > 0$ such that $B_2(c,r) = B_2(c, \sqrt{r^2+\varepsilon})$. This can be done since for all $x \notin B_2(c,r)$, $d_2(c,x) > r$. Note that

$$d_2(c,x)^2 - \|c\|_2^2 = \sum_{x_i=1}(1-2c_i) = \sum_{x_i=1}(2\overline{c}_i - 1) = \|\overline{c}\|_2^2 - d_2(\overline{c},x)^2,$$

so that $d_2(c,x) \le r$ implies $d_2(\overline{c},x)^2 \ge \|\overline{c}\|_2^2 + \|c\|_2^2 - r^2$ and thus $x \notin B_2(\overline{c},r)$. Furthermore, $d_2(c,x) > \sqrt{r^2+\varepsilon}$ implies that $d_2(\overline{c},x)^2 < \|\overline{c}\|_2^2 + \|c\|_2^2 - r^2 - \varepsilon$ and thus $x \in B_2(\overline{c},r)$.

For d) an easy calculation yields $\|m\vec{\jmath} - \varepsilon q\|_1 = mk - \varepsilon(1-2^{-k})$, so that the formula follows from

$$\begin{aligned} d_1(m\vec{\jmath} - \varepsilon q, b(n)) - \|m\vec{\jmath} - \varepsilon q\|_1 &= \sum_{b(n)_i=1} f_1(m\vec{\jmath} - \varepsilon q) = \sum_{b(n)_i=1}(1-2m+\varepsilon 2^{1-i}) \\ &= (1-2m)w(b(n)) + \varepsilon 2^{1-k}\sum_{b(n)_i=1} 2^{k-i} = (1-2m)w(b(n)) + \varepsilon 2^{1-k} n. \end{aligned}$$

e) follows from d) by setting $m = 1/2$ and $\varepsilon = 1$, since then $d_1(c,x) = \|c\|_1 + n2^{1-k}$, which is increasing in n. For f) setting $m = 1/4$ and $\varepsilon = 1/2$, we obtain $d_1(c,x) = \|c\|_1 + \frac{1}{2}[w(b(n)) + n2^{-k}]$. Since $n < 2^k$ for all $b(n) \in \{0,1\}^k$, we have $x \in B$ if $w(x) < t$ and $x \notin B$ if $w(x) > t$. If $w(x) = t$, then $x \in B$ if and only if it is lexicographically no bigger than y. $\square$

So discrete balls have all the properties we expect of a candidate for extremal sets. In fact, we

Conjecture. *For every (n,k) some extremal set is a discrete ball.*

So far *every* known good construction is a discrete ball and discrete balls are also the solutions to other isoperimetric problems, like those in [AK, BL, H, Ht, Ka2]. There are product constructions that in some cases beat both the cube and the sphere, but even those are discrete balls.

Definition 6. For $S \subset \{0,1\}^j$ and $T \subset \{0,1\}^{k-j}$ we define their *cartesian product* $S \times T \subset \{0,1\}^k$ as $\{(s_1, s_2, \ldots, s_j, t_1, t_2, \ldots, t_{k-j}) : s \in S, t \in T\}$.

Proposition 5.

a) $d(S \times T) = |T|^2 d(S) + |S|^2 d(T)$.

b) $Q_{k-j}(n) \times \{0,1\}^j = Q_k(n2^j)$ *and* $\{0_j\} \times Q_{k-j}(n) = Q_k(n)$.

c) For $c \in \mathbb{R}^{k-j}$, $B_1(c,r) \times \{0,1\}^j = B_1(\overline{c}, r+j/2)$, *where* $\overline{c}_i = c_i$ *if* $i \le k-j$ *and* $\overline{c}_i = 1/2$ *if* $k-j < i \le k$. *The k-dimensional ball is a right-shifted down-set if and only if the $(k-j)$-dimensional one is.*

d) For $c \in [0,1/2]^{k-j}$, $\{0_j\} \times B_1(c,r) = B_1(\overline{c},r)$ if and only if $r < \|c\|_1 + 1$, where $\overline{c}_i = c_i$ if $j < i \le k$ and $\overline{c}_i = 0$ if $i \le j$. The k-dimensional ball is a right-shifted down-set if and only if the $(k-j)$-dimensional one is.

Proof. a) follows from (1) and b) is straight forward. For c) we observe that for $x \in \{0,1\}^k$, $d_1(\overline{c},x) = d_1(c,(x_1,\dots x_{k-j})) + j/2$. The second parts of c) and d) follow from Proposition 4b). For d) note that for $x \in \{0,1\}^j$ and $y \in \{0,1\}^{k-j}$, $d_1(\overline{c},(x,y)) = w(x)+d_1(c,y)$. Thus if $w(x) = 0$, then $(x,y) \in B_1(\overline{c},r)$ exactly when $y \in B_1(c,r)$. If $w(x) > 0$, then $d_1(\overline{c},(x,y)) \ge 1 + \|c\|_1$, so that $(x,y) \notin B_1(\overline{c},r)$ exactly if $r < \|c\|_1 + 1$.

For example, if $S = B((0,0,0,0,0,0,0,0,1/2,1/2),2) = B_8(9) \times \{0,1\}^2$, then $d(S) = 4^2 \cdot 64 + 9^2 \cdot 8 = 1672$, whereas $d(Q_{10}(36)) = 1736$ and $d(B_{10}(36)) = 1730$. It can also be shown that no other generalized Hamming sphere has distance sum at most 1672, so that this product beats both the sphere and the cube.

4. Recognizing discrete balls

To decide whether a given set is a discrete ball, we first bring it into standard form. Then we can determine its set of generators and solve a system of linear inequalities as described in this section to determine whether it is indeed a discrete ball.

Definition 7. The right-shifted down-set *generated by* a set $G \subset \{0,1\}^k$, denoted by $RD(G)$, is the smallest right-shifted down-set containing G. It can be found as the intersection of all right-shifted down-sets containing G. $LU(G)$ is defined similarly.

The *generator* for a set S, denoted by $G(S)$, is the set of all $x \in S$, such that $x \notin RD(S - x)$. We similarly define $G^+(S)$ for LU.

It can be seen that $RD(G(S)) = RD(S)$ and that $G(S)$ is the unique minimal set generating $RD(S)$. Furthermore, S is a right-shifted down-set if and only if $S = RD(S)$ and $RD(G) = \bigcup_{g \in G} RD(\{g\})$. Since $G^+(S) = r(G(r(S)))$, similar statements hold for left-shifted up-sets.

Theorem 6. *The following are equivalent*

a) S is a discrete ball in standard form

b) The system of linear inequalities

$$\sum_{x_i=1} z_i \le 1 \text{ for all } x \in G(S)$$
$$\sum_{x_i=1} z_i > 1 \text{ for all } x \in G^+(\overline{S})$$

has a solution with $z_1 \ge z_2 \ge \cdots \ge z_k \ge 0$.

Proof. If S is a discrete ball in standard form, then $0 \in S$ and we can assume that $0 \le c_1 \le c_2 \le \cdots \le c_k \le 1/2$. Thus $r \ge d_1(0,c) = \|c\|_1$, and by an argument like in the proof of Proposition 4c) we can assume that the inequality is strict. Now set

$$z_i := \frac{1-2c_i}{r-\|c\|_1}.$$

Certainly $z_1 \geq z_2 \geq \cdots \geq z_k \geq 0$ and the remaining inequalities correspond to

$$\sum_{x_i=1} f_1(c_i) \leq r - \|c\|_1 \text{ for all } x \in G(S) \subset S$$
$$\sum_{x_i=1} f_1(c_i) > r - \|c\|_1 \text{ for all } x \in G^+(\overline{S}) \subset \overline{S}$$

which are also satisfied.

Conversely, suppose that the inequalities in b) have the specified solution. It suffices to show that $S = B_2(c,r)$, where $c_i = (1-z_i)/2$ and $r = \sqrt{1+\|c\|_2^2}$. For all $x \in \{0,1\}^k$

$$d_2(x,c)^2 - \|c\|_2^2 = \sum_{x_i=1} f_2(c_i) = \sum_{x_i=1} z_i.$$

For every $x \in S$ there is a $y \in G(S)$ with $x \in RD(y)$. So if $\{i : x_i = 1\} = \{i_1, i_2, \ldots i_r\}$ and $\{j : y_j = 1\} = \{j_1, j_2, \ldots j_s\}$, then $i_\ell \geq j_\ell$ for all $1 \leq \ell \leq r$. Hence

$$d_2(x,c)^2 - \|c\|_2^2 = \sum_{x_i=1} z_i = \sum_{1\leq \ell \leq r} z_{i_\ell} \leq \sum_{1\leq \ell\leq r} z_{j_\ell} \leq \sum_{y_j=1} z_j \leq 1,$$

and $x \in B_2(c,r)$. Similarly, for $x \in \overline{S}$ there is a $y \in G^+(\overline{S})$ with $x \in LU(y)$. Here, in the notation from above, $i_\ell \leq j_\ell$ for all $1 \leq \ell \leq s$. So

$$d_2(x,c)^2 - \|c\|_2^2 = \sum_{x_j=1} z_j \geq \sum_{1\leq \ell\leq s} z_{i_\ell} \geq \sum_{1\leq \ell \leq s} z_{j_\ell} = \sum_{y_i=1} z_i > 1,$$

and $x \notin B_2(c,r)$. $\square$

We can now easily see that for example $S = RD(110000, 001111)$ is not a discrete ball. We observe that $\overline{S} = LU(010011)$ and S is in standard form, so that it is a discrete ball if and only if the system

$$\begin{aligned} z_1 + z_2 &\leq 1 \\ z_3 + z_4 + z_5 + z_6 &\leq 1 \\ z_2 + z_5 + z_6 &> 1 \end{aligned}$$

has a solution with $z_1 \geq z_2 \geq z_3 \geq z_4 \geq z_5 \geq z_6 \geq 0$. However, this would imply that $z_2 \leq 1/2$ and $z_5 + z_6 \leq 1/2$, a contradiction. Note that S is not an extremal set.

4. Small values

It follows from Theorem 1 that if $n \leq 8$, then $f(n,k) = (n-1)^2$, except that $f(4,k) = 8$ and $f(8,k) = 48$. Furthermore, $Q_k(n)$ is an extremal set and the only other standard extremal sets in this range are $B_k(n)$ for $5 \leq n \leq 7$ and $n \leq k+1$. By complementation the corresponding statements hold for $n \geq 2^k - 8$, so that for $k \leq 4$ the situation is fully characterized. Also recall that $Q_k(n) = B_k(n)$ if and only if $n \leq 3$ or $n \geq 2^k - 3$.

Table 1 lists all the values of $f(n,k)$ for $9 \leq n \leq 18$. The subscript indicates the number of extremal sets in standard form – if there is no subscript then the extremal set is unique. For example, there are exactly 5 distinct standard extremal sets achieving $f(11,7) = 112$. Note that for $k \geq 17 \geq n$, $f(n,k) = f(n,16)$, and that $f(18,k) = 289$ for $k \geq 17$.

$n \setminus k$	4	5	6	7	8	9	10	11	12	13	14	15	16
9	68	68	68	68_2	64	64	64	64	64	64	64	64	64
10	89	89_2	89_2	89_3	86	81	81	81	81	81	81	81	81
11	112_2	112_2	112_3	112_5	110	106	100	100	100	100	100	100	100
12	136	136	136_2	136_2	136_4	133	128	121	121	121	121	121	121
13	164	164	164	164_2	164_3	162_2	158	152	144	144	144	144	144
14	193	193	193	193_2	193_2	193_3	190_2	185	178	169	169	169	169
15	224	224	224	224	224	224	224_2	220_2	214	206	196	196	196
16	256	256	256	256	256	256	256	256	252_2	245	236	225	225
17	–	304	304	304	304	298	298_2	296	292	286_2	278	268	256
18	–	353	353	353	353_2	337	337	337_2	334	329	322_2	313	302

Table 1: Values of $f(n,k)$ for $9 \leq n \leq 18$.

n	$Q_k(n)$	$B_k(n)$	Generators for other standard extremal sets
9	$k \leq 7$	$k \geq 7$	none
10	$k \leq 7$	$k \geq 7$	$U_5,\ U_6,\ U_7$
11	$k \leq 7$	$k \geq 7$	$\{e_{k-3} + e_{k-2}\}(k \leq 7),\ T_6^1,\ T_7^1,\ T_7^2$
12	$k \leq 8$	$k \geq 8$	$U_6,\ U_7,\ U_8,\ T_8^1$
13	$k \leq 8$	$k \geq 9$	$T_7^1,\ T_8^1,\ T_8^2,\ T_9^1$
14	$k \leq 9$	$k \geq 10$	$U_7,\ U_8,\ U_9,\ T_9^1,\ T_{10}^1$
15	$k \leq 10$	$k \geq 11$	$T_{10}^1,\ T_{11}^1$
16	$k \leq 11$	$k \geq 12$	T_{12}^1
17	$k \leq 8$	$k \geq 13$	$T_k^1(9 \leq k \leq 13), T_{10}^2$
18	$k \leq 8$	$k \geq 14$	$\{00000111, 10000001\},\ U_9,\ U_{10},\ U_{11},\ T_k^1(11 \leq k \leq 14)$

Table 2: Standard extremal sets for $9 \leq n \leq 18$.

Table 2 lists all standard extremal sets corresponding to the entries in Table 1. As usual, let $e_i := r_i(0)$ denote the standard basis vectors. For simplicity, define the following generators in $\{0,1\}^k$:

$$U_k(n) = \{e_k + e_{k+1-n/2}\} \text{ for even } n \le 2k,$$
$$T_k^r(n) = \{e_r, e_k + e_{2k+2-r-n}\} \text{ for } 1 \le r < 2k+2-r-n < k.$$

For example $T_8^2(13) = \{01000000, 00100001\}$, and we can drop the argument since there is no ambiguity.

Observe that the extremal set for $(18,8)$ is the smallest such set that is neither a sphere nor a cube – however, it is the discrete ball $B_1((0,0,0,0,0,1/4,1/4,1/2),2)$. Although it is true that for $k \ge n-1$ spheres are extremal, Table 2 is misleading since in general it is not the case that for small k cubes are extremal: By Proposition 3 and Theorem 1 the cube is not extremal for $n = 2^k - 9$ if $k \ge 8$. We believe that for $k \le 7$ the cube is optimal for all $n \le 2^k$.

5. Choosing the center

Although there are fewer discrete balls than right-shifted down-sets, there are still many of them. Maybe the conjecture can be sharpened by requiring additional properties of the discrete balls, like its center is of the form $m\vec{\jmath} - \varepsilon q$ as suggested by Proposition 4d)-f).

Definition 8. The *centroid* of a set $S \subset \{0,1\}^k$ is defined as

$$c(S) := |S|^{-1} \sum_{x \in S} x = (w_1(S)/|S|, w_2(S)/|S|, \ldots, w_k(S)/|S|).$$

The set S is called a *good ball* if $S = B_1(c(S), r)$ for some $r \ge 0$, or equivalently by Theorem 5b), if $S = B_2(c(S), r)$ for some $r \ge 0$.

Proposition 6.
a) $d(S) = |S|^2 c(S) \cdot (\vec{\jmath} - c(S))$.
b) If S is a good ball, then $r_i(S)$, $s_{ij}(S)$ and $\overline{S}$ are good balls.
c) $B(0,r)$ is a good ball.

Proof. a) is just a rewriting of (1). By observing that $r_i(c(S)) = c(r_i(S))$ and $s_{ij}(c(S)) = c(s_{ij}(S))$, the first two assertions in b) follow from the proof of Proposition 4a). If we define for any set S and $x \in \{0,1\}^k$

$$S(x) = \sum_{x_i = 0} w_i(S) + \sum_{x_i = 1} (|S| - w_i(S)),$$

then a quick calculation yields $\overline{S}(x) = k2^{k-1} - S(x)$ and $d_1(x, c(S)) = S(x)/|S|$. So if $S = B_1(c(S), r)$, where $r \ge 0$ is such that $S = B_1(c(S), r - \varepsilon)$ for some $\varepsilon > 0$, then it follows easily, that $\overline{S} = B_1(c(\overline{S}), (k2^{k-1} - r|S|)/(2^k - |S|)$.

The proof of c) is straight forward, since $c(B(0,r)) = y\vec{\jmath}$ with $0 \le y \le r/k$. □

It is also worth noting that all standard extremal sets mentioned in Section 4 and Theorems 1-3 are good balls. In short, all known extremal sets are good balls. However, not all discrete balls are good balls: $S = RD(e_2, e_7 + e_8) \subset \{0,1\}^9$ has $\overline{S} = LU(e_1, e_6{+}e_9, e_7{+}e_8{+}e_9)$ and is a discrete ball, since the corresponding system has a solution ($z_1 = 2$, $z_2 = \cdots = z_6 = 1$ and $z_7 = z_8 = z_9 = 1/2$). Its centroid is $c(S) = \frac{1}{12}(0,1,1,1,1,1,3,3,3)$ and $d(c(S), e_7 + e_8) = 26/12 = d(c(S), e_1)$, so that S is not a good ball.

Question. *Is some/every extremal set achieving $f(n,k)$ a good ball?*

Acknowledgments. The author is grateful to Mitch Harris and Jeff Erickson, who suggested looking at discrete balls, and Levon Khachatrian, Ken Zeger, Radhika Ramamurthi and Zoltán Füredi for helpful remarks. The computer program that generated the values for the tables was written by Christian Deppe.

References

[AA] R. Ahlswede, I. Althöfer, *The asymptotic behaviour of diameters in the average*, J. Combin. Theory Ser. B **61** (1994), 167–177.

[AK] R. Ahlswede, G. O. H. Katona, *Contributions to the geometry of Hamming spaces*, Discrete Math. **17** (1977), 1–22.

[AS] I. Althöfer, T. Sillke, *An "average distance" inequality for large subsets of the cube*, J. Combin. Theory Ser. B **56** (1992), 296–301.

[Bz] S. L. Bezrukov, *Isoperimetric problems in discrete spaces*, Bolyai Soc. Math. Stud. **3** (1994), 59–91.

[Bl] W. Blaschke, *Eine isoperimetrische Eigenschaft des Kreises*, Math. Z. **1** (1918), 52–57.

[BL] B. Bollobas, I. Leader, *Maximal sets of given diameter in the grid and the torus*, Discrete Math. **122** (1993), 15–35.

[FF] P. Frankl, Z. Füredi, *A short proof for a theorem of Harper about Hamming-spheres*, Discrete Math. **34** (1981), no. 3, 311–313.

[F] F. Fu, *On the improvements of Althöfer-Sillke inequality*, J. Math. Res. Exposition **16** (1996), no. 3, 325–328.

[FWY] F. Fu, V. R. Wei, R. W. Yeung, *On the minimum average distance of binary codes: Linear programming approach*, preprint (1999).

[H] L. H. Harper, *Optimal numberings and isoperimetric problems*, J. Combinatorial Theory **1** (1966), 385–393.

[Ht] S. Hart, *A note on the edges of the n-cube*, Discrete Math. **14** (1976), 157–163.

[JKM] F. Jaeger, A. Khelladi, M. Mollard, *On shortest cocyle covers of graphs*, J. Combin. Theory Ser. B **39** (1985), 153–163.

[JT] U. Jamshy, M. Tarsi, *Cycle covering of binary matroids*, J. Combin. Theory Ser. B **46** (1989), 154–161.

[Ka1] G. O. H. Katona, *The Hamming-sphere has minimum boundary*, Studia Sci. Math. Hungar. **10** (1975), no. 1–2, 131–140.

[Ka2] G. Katona, *Intersection theorems for systems of finite sets*, Acta Math. Acad. Sci. Hungar **15** (1964), 329–337.

[K] A. Kündgen, *Covering cliques with spanning bicliques*, J. Graph Theory **27** (1998), no. 4, 223–227.

[S] L. A. Santaló, *Integral geometry and geometric probability*, Encyclopedia of Mathematics and its Applications, Vol.1, Addison-Wesley Publishing Co., Reading,Mass.-London-Amsterdam, 1976.

[T] M. Tarsi, *Nowhere zero flow and circuit covering in regular matroids*, J. Combinatorial Theory, Ser. B **39** (1985), 346–352.

[XF] S. Xia, F. Fu, *On the average Hamming distance for binary codes*, Discrete Appl. Math. **89** (1998), 269–276.

Department of Mathematics, University of Illinois, Urbana, Illinois 61801
E-mail address: kundgen@member.ams.org