Discrete Mathematics 51 (1984) 147-165
North-Holland

ODD AND EVEN HAMMING SPHERES ALSO HAVE MINIMUM BOUNDARY

Janos KÖRNER* and Victor K. WEI
Bell Laboratories, Murray Hill, NJ 07974, USA

Received 16 April 1982
Revised 27 June 1983

Combinatorial problems with a geometric flavor arise if the set of all binary sequences of a fixed length n, is provided with the Hamming distance. The *Hamming distance* of any two binary sequences is the number of positions in which they differ. The (outer) boundary of a set $\mathbf{A}$ of binary sequences is the set of all sequences outside $\mathbf{A}$ that are at distance 1 from some sequence in $\mathbf{A}$. Harper [6] proved that among all the sets of a prescribed volume, the 'sphere' has minimum boundary.

We show that among all the sets in which no pair of sequences have distance 1, the set of all the sequences with an even (odd) number of 1's in a Hamming 'sphere' has the same minimizing property. Some related results are obtained. Sets with more general extremal properties of this kind yield good error-correcting codes for multi-terminal channels.

1. Preliminaries

The set of all binary sequences of a fixed length, n, say, is often looked at as a metric space, with the distance of any two sequences being the number of positions in which they differ. This is known as *Hamming distance*. Formally, set $\mathbf{X}=\{0, 1\}$. Then $\mathbf{X}^n$ is the set of all binary sequences of length n The Hamming distance $d(\mathbf{x}, \mathbf{y})$ of any two sequences $\mathbf{x}\in\mathbf{X}^n$, $\mathbf{y}\in\mathbf{X}^n$ is

$$d(\mathbf{x}, \mathbf{y}) := \sum_{i=1}^{n} |x_i - y_i|, \qquad \text{where } \mathbf{x} = x_1 \cdots x_n, \quad \mathbf{y} = y_1 \cdots y_n.$$

For two subsets $\mathbf{A}$ and $\mathbf{B}$ of $\mathbf{X}^n$, the distance $d(\mathbf{A}, \mathbf{B})$ is defined correspondingly as the smallest distance $d(\mathbf{x}, \mathbf{y})$ between any pair of sequences $\mathbf{x}\in\mathbf{A}$, $\mathbf{y}\in\mathbf{B}$. (The same set $\mathbf{X}^n$ is usually interpreted as the family of all the subsets of a given set of n distinct elements. Then every binary sequence is considered as the characteristic function of a particular subset. Further, the Hamming distance of two sequences is the cardinality of the symmetric difference of the subsets they represent.)

This set-up leads to interesting problems in combinatorics that have a certain geometric flavor. Our aim is to generalize a result of Harper [6] which can be considered as a discrete analogue of the isoperimetric problem of classical geometry.

* On leave from the Mathematical Institute of the Hungarian Academy of Sciences, Budapest.

0012-365X/84/$3.00

For every positive integer d introduce the operation Γ^d on subsets of $\mathbf{X}^n$. For $\mathbf{A}\subset\mathbf{X}^n$, $\Gamma^d\mathbf{A}$ is the set of those elements in $\mathbf{X}^n$ that are at distance at most d from some element of $\mathbf{A}$. Thus

$$\Gamma^d\mathbf{A}:=\{\mathbf{x}: \mathbf{x}\in\mathbf{X}^n, d(\{\mathbf{x}\},\mathbf{A})\leq d\}.$$

Clearly, $\Gamma^d\mathbf{A}=\Gamma(\Gamma^{d-1}\mathbf{A})$. In particular, for $\Gamma:=\Gamma^1$, the set $\Gamma\mathbf{A}-\mathbf{A}$ is called the *outer boundary* of $\mathbf{A}$. The set $\Gamma^d\{\mathbf{x}\}$ is called a *Hamming sphere* with *radius* d and *center* $\mathbf{x}$. This kind of Hamming sphere have 'volumes' $|\Gamma^d\{\mathbf{x}\}|$ that are equal to

$$\sum_{i=0}^{d}\begin{bmatrix} n \\ i \end{bmatrix}. \tag{1}$$

For a number k that is between these sums of binomial coefficients for d and $d+1$, say, the 'Hamming sphere with volume k and center $\mathbf{x}$' will be defined as an arbitrary k-element subset of $\Gamma^{d+1}\{\mathbf{x}\}$, containing $\Gamma^d\{\mathbf{x}\}$. Harper [6] proved that among all the subsets $\mathbf{A}\subset\mathbf{X}^n$ of given cardinality ('volume'), the cardinality of the outer boundary ('surface') is minimized by a Hamming-sphere. Recently, a very nice simple proof of Harper's result was found by Frankl and Füredi [5]. In their formulation, the result says that

Theorem H. *To any subsets* $\mathbf{A}$ *and* $\mathbf{B}$ *of* $\mathbf{X}^n$ *there exists a Hamming sphere,* $\hat{\mathbf{A}}$, *centered at the all-zero sequence and another one,* $\hat{\mathbf{B}}$, *centered at the all-one sequence such that*

$$|\hat{\mathbf{A}}|=|\mathbf{A}|,\quad |\hat{\mathbf{B}}|=|\mathbf{B}|,\qquad d(\hat{\mathbf{A}},\hat{\mathbf{B}})\geq d(\mathbf{A},\mathbf{B}). \tag{2}$$

This means that two 'antipodal' Hamming spheres are more distant than any pair of sets with the same pair of cardinalities. (In order to see that this implies Harper's result, consider an arbitrary set $\mathbf{A}$ and choose $\mathbf{B}$ to be complement of $\Gamma\mathbf{A}$. Then $d(\mathbf{A},\mathbf{B})=2$. Theorem H gives us Hamming spheres $\hat{\mathbf{A}}$, $\hat{\mathbf{B}}$ such that $d(\hat{\mathbf{A}},\hat{\mathbf{B}})\geq 2$ and $|\hat{\mathbf{A}}|=|\mathbf{A}|$, $|\hat{\mathbf{B}}|=|\mathbf{B}|=2^n-|\Gamma\mathbf{A}|$. Thus $\Gamma\hat{\mathbf{A}}$ and $\hat{\mathbf{B}}$ are disjoint, and we have

$$|\Gamma\hat{\mathbf{A}}|\leq 2^n-|\hat{\mathbf{B}}|=2^n-|\mathbf{B}|=|\Gamma\mathbf{A}|.$$

The other implication can be shown similarly.)

Harper's proof is simple and settles the isoperimetric problem for cardinalities k of form (1). Looking at the problem more closely, however, one sees that if k cannot be written into the form (1), not all the Hamming spheres have the same outer boundary. Harper's Theorem 1 in [6] actually describes an algorithm that yields Hamming spheres of minimum outer boundary for arbitrary volumes k. Implicit in his result is a rather simple proof of a well-known result of Kruskal and Katona. In fact, the latter is needed to calculate the cardinality of the minimum outer boundary. (For various proofs of the Kruskal–Katona theorem, cf. Kruskal [9], Katona [7], and Eckhoff–Wegner [4].) In order to quote Kruskal–Katona theorem, observe first that

Lemma K. *For any given positive integers m and p the number m has a representation*

$$m=\binom{a_p}{p}+\binom{a_{p-1}}{p-1}+\cdots+\binom{a_r}{r} \tag{3}$$

such that

$$a_p>a_{p-1}>\cdots>a_r\geq r\geq 1.$$

Moreover this representation is unique.

Formula (3) is called the *p-canonical representation of m*. Kruskal introduced a function F, setting

$$F(m,p)=\binom{a_p}{p-1}+\binom{a_{p-1}}{p-2}+\cdots+\binom{a_r}{r-1}, \tag{4}$$

where the a_p's are the same as in (3). (Notice that formula (4) gives $F(m,p)$ in its $(p-1)$-canonical representation whenever $r>1$ in (3).)

Denote by $\mathbf{W}_p$ the set of all binary sequences with exactly p 1's, i.e.,

$$\mathbf{W}_p:=\left\{\mathbf{x}: \mathbf{x}\in\mathbf{X}^n, \sum_{i=1}^{n} x_i=p\right\}.$$

Kruskal proved that

Theorem K. *For any $\mathbf{A}\subset\mathbf{W}_p$ with $|\mathbf{A}|=m$ one has $|\Gamma\mathbf{A}\cap\mathbf{W}_{p-1}|\geq F(m,p)$, and this lower bound is optimal.*

For later purposes, we include here a lemma of Eckhoff and Wegner [4] that gives a recursive relation for Kruskal's function.

Lemma EW

$$F(m_0+m_1,p)\leq\max[m_0,F(m_1,p)]+F(m_0,p-1). \tag{5}$$

Combining the results of Harper and Krustal one arrives at the more precise result of Katona [8]. First we need his

Lemma HK. *Any integer m with $0<m<2^n$ has a unique representation*

$$m=\binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{p'}+\binom{a_{p'-1}}{p'-1}+\binom{a_{p'-2}}{p'-2}+\cdots+\binom{a_{r'}}{r'} \tag{6}$$

such that

$$n>a_{p'-1}>a_{p'-2}>\cdots>a_{r'}\geq r'\geq 1,$$

and this representation is unique.

This lemma is an easy consequence of Lemma K. In (6), p' is the unique integer for which

$$\sum_{i=p'}^{n}\binom{n}{i}\leq m<\sum_{i=p'-1}^{n}\binom{n}{i}. \tag{7}$$

Further, the right-hand side of (6) is the sum of $\sum_{i=p'}^{n}\binom{n}{i}$ and the $(p'-1)$-canonical representation of $m-\sum_{i=p'}^{n}\binom{n}{i}$. Katona calls (6) the *n-bounded canonical representation of m*. Introduce now

$$G(m,n):=\binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{p'-1}+\binom{a_{p'-1}}{p'-2}$$
$$+\binom{a_{p'-2}}{p'-3}+\cdots+\binom{a_{r'}}{r'-1}. \tag{8}$$

Clearly, if m satisfies (7), then

$$G(m,n)=\sum_{i=p'-1}^{n}\binom{n}{i}+F\left(m-\sum_{i=p'}^{n}\binom{n}{i},p'-1\right).$$

The isoperimetric property of the Hamming sphere amounts to

Theorem HK. *Given any positive integer m with $m<2^n$, the cardinality of the outer boundary of any m-element subset of $\mathbf{X}^n$ is at least $G(m,n)-m$. Further, $G(m,n)-m$ is the exact cardinality of the outer boundary of a certain Hamming sphere.*

The minimum is achieved for a Hamming sphere in which the sequences having maximum distance from the center are chosen to yield the exact minimum in the Kruskal–Katona theorem. However, an m-element set having minimum boundary is not necessarily a Hamming sphere. An example is given in Appendix B.

Katona also proved the following: Write

$$G_d(m,n):=\binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{p'}+\binom{n}{p'-1}+\cdots+\binom{n}{p'-d}$$
$$+\binom{a_{p'-1}}{p'-d-1}+\binom{a_{p'-2}}{p'-d-2}+\cdots+\binom{a_{r'}}{r'-d} \tag{9}$$

where the a's are as in (6). The understanding is that in (9) we omit the terms for which $r'<d$. Then we have

Theorem KH. *Given any positive integer m with $m<2^n$, the cardinality of the d-Hamming neighborhood, $\Gamma^d\mathbf{A}$, of sets $\mathbf{A}\subset\mathbf{X}^n$ satisfying $|\mathbf{A}|=m$ is at least $G_d(m,n)$. Further, the minimum is achieved by a certain Hamming sphere.*

Various generalization of Theorem KH play an interesting role in information theory. Katona's paper [8] was motivated by an asymptotic answer to a probabilistic generalization of the isoperimetric problem given by Margulis [10], Ahlswede–Gacs–Körner [1], cf. also Csiszár–Körner [3].

2. Results

In this paper we are concerned with purely combinatorial generalizations of the isoperimetric problem. The nature of our generalization is to look for the set $\mathbf{A} \subset \mathbf{X}^n$ that minimizes the size of the outer boundary (or more generally, of the d-neighborhood) for a fixed $|\mathbf{A}|$, within a restricted family of subsets of the set of all binary sequences, $\mathbf{X}^n$.

These problems arise naturally in an information-theoretic context. In their attempt to devise good error correcting codes for the so-called broadcast channel, Bassalygo et al. [2] needed an estimate on the smallest possible size of the d-neighborhood of e-error correcting codes $\mathbf{A}$ with given size (A set $\mathbf{A} \subset \mathbf{X}^n$ is an e-error correcting code if any two elements of $\mathbf{A}$ have Hamming distance strictly greater than $2e$).

For any set $\mathbf{A} \subset \mathbf{X}^n$, define the *hole-diameter*, $d(\mathbf{A})$, of $\mathbf{A}$ to be the minimum distance among different elements of $\mathbf{A}$. Motivated by the above, we ask

Problem. Given positive integers d', $d<n$ and $m<2^n$, what is the smallest possible size of the d-neighborhood of sets $\mathbf{A} \subset \mathbf{X}^n$ with hole-diameter d' and $|\mathbf{A}| = m$.

The case of $d'=1$ and arbitrary d is settled by the Harper–Kruskal–Katona result: Theorem KH. It is clear that if d' is large enough with respect to d, then the problem is essentially solved. Namely, if $d' \geqslant 2d+1$, then the elements of any set $\mathbf{A}$ with hole diameter at least d' have disjoint d-neighborhoods, and therefore

$$|\Gamma^d \mathbf{A}| = |\mathbf{A}| \sum_{i=0}^{d} \binom{n}{i}.$$

The only open question in such a case is to decide how big $|\mathbf{A}|$ can be. The latter is a very difficult open problem in coding theory, cf. McEliece et al. [12] and the book of MacWilliams–Sloane [11].

In what follows, we will solve the above problem for an arbitrary d in the case $d'=2$. More precisely, we will prove the corresponding generalizations of Theorems H and HK.

We will say that $\mathbf{A}$ is a *pure-parity set* if the sum $\sum_{i=1}^{n} x_i$ of the coordinates has the same parity for every element $\mathbf{x} = (x_1 x_2 \cdots x_n)$ of $\mathbf{A}$. We shall say that $\mathbf{A}$ is an *odd- (even-) parity set* if this parity is odd (even). An *odd- (even-) parity Hamming sphere* is simply the largest odd (even) set contained in a Hamming sphere. A *pure-parity Hamming sphere* is either an odd- or an even-parity

Hamming sphere. The core of our results is

Theorem 1. *To every pair of subsets, $\mathbf{A}$, $\mathbf{B}$, of $\mathbf{X}^n$ where $\mathbf{A}$ is of pure parity and $\mathbf{B}$ is arbitrary, there exists a pure-parity Hamming sphere $\mathbf{A}'$ having the same parity as $\mathbf{A}$ and a set $\mathbf{B}'$ such that*

$$|\mathbf{A}'|=|\mathbf{A}|,\quad |\mathbf{B}'|=|\mathbf{B}|,\qquad d(\mathbf{A}',\mathbf{B}')\geq d(\mathbf{A},\mathbf{B}).$$

The proof of this theorem is based on the ideas of Frankl and Füredi [5]. Using the Kruskal–Katona theorem, Theorem 1 allows us to determine the smallest cardinality of the outer boundary of any pure-parity set of prescribed cardinality. To this end, we note

Lemma 1. *Any positive integer m with $m\leq 2^{n-1}$ has a unique representation in the form*

$$m=\binom{n}{n}+\binom{n}{n-2}+\cdots+\binom{n}{n-2k+2}+m', \tag{10a}$$

where

$$m'=\binom{a_{n-2k}}{n-2k}+\binom{a_{n-2k-1}}{n-2k-1}+\cdots+\binom{a_s}{s}, \tag{10b}$$

with $n>a_{n-2k}>a_{n-2k-1}>\cdots>a_s\geq s\geq 1$. Further, m has a unique representation in the form

$$m=\binom{n}{n-1}+\binom{n}{n-3}+\cdots+\binom{n}{n-2l+1}+m'', \tag{11a}$$

where

$$m''=\binom{b_{n-2l-1}}{n-2l-1}+\binom{b_{n-2l-2}}{n-2l-2}+\cdots+\binom{b_t}{t}, \tag{11b}$$

with $n>b_{n-2l-1}>b_{n-2l-2}>\cdots>b_t\geq t\geq 1$.

Call (10) the *n-matched representation of m*, and (11) the *n-mismatched representation of m*. Set

$$\varphi^*(m,n)=\binom{n}{n-1}+\binom{n}{n-3}+\cdots+\binom{n}{n-2k+1}+F(m',n-2k),$$

$$\varphi^{**}(m,n)=\binom{n}{n}+\binom{n}{n-2}+\cdots+\binom{n}{n-2l}+F(m'',n-2l-1).$$

Note that

$$F(m',n-2k)=\binom{a_{n-2k}}{n-2k-1}+\binom{a_{n-2k-1}}{n-2k-2}+\cdots+\binom{a_s}{s-1},$$

$$F(m'',n-2l-1)=\binom{b_{n-2l-1}}{n-2l-2}+\binom{b_{n-2l-2}}{n-2l-3}+\cdots+\binom{b_t}{t-1}.$$

In the next section, we show that

Lemma 2. *For every* $m \leqslant 2^{n-1}$, *we have*

$$\varphi^*(m, n) = \varphi^{**}(m, n).$$

It is easy to see that, for every $m \leqslant 2^{n-1}$, there exists an m-element subset $\mathbf{A}$ of $\mathbf{X}^n$ of either odd or even parity such that $\Gamma\mathbf{A} - \mathbf{A}$ has $\varphi^*(m, n) = \varphi^{**}(m, n)$ elements. Let $\varphi(m, n)$ denote the minimum cardinality of the outer boundary of m-element subsets of $\mathbf{X}^n$ with hole-diameter at least two, i.e.

$$\varphi(m, n) := \min_{\substack{|\mathbf{A}|=m \\ d(\mathbf{A}) \geqslant 2}} |\Gamma\mathbf{A} - \mathbf{A}|.$$

We shall prove that $\varphi(m, n) = \varphi^*(m, n) = \varphi^{**}(m, n)$. We need one more lemma.

Lemma 3. *If* $\mathbf{A}_0$ *has minimum outer boundary among all* m*-element subsets of* $\mathbf{X}^n$ *with hole-diameter greater than or equal to two, i.e.* $|\mathbf{A}_0| = m$, $d(\mathbf{A}_0) \geqslant 2$, *and* $|\Gamma\mathbf{A}_0 - \mathbf{A}_0| = \varphi(m, n)$, *then all elements of* $\mathbf{A}_0$ *have the same parity.*

Theorem 2. *For every* $m \leqslant 2^{n-1}$, *we have*

$$\varphi(m, n) = \varphi^*(m, n) = \varphi^{**}(m, n).$$

We shall present two proofs to Theorem 2. One proof, which uses Theorem 1, the above lemmas, and the Kruskal–Katona theorem is presented in the next section. The other proof, which uses the Eckhoff–Wegner technique [4], is presented in Appendix A.

We remark here that $\varphi^*(m, n)$ is exactly the size of the outer boundary of an even-parity Hamming sphere whose outermost layer is chosen according to the Kruskal–Katona scheme. Hence such an even-parity Hamming sphere achieves minimum outer boundary $\phi(m, n)$. Similarly, there are odd-parity Hamming spheres that achieve minimum outer boundary $\varphi^{**}(m, n) = \varphi(m, n)$. Extending our previous results, we obtain

Theorem 3. *Given any positive integer* $m \leqslant 2^{n-1}$, *the cardinality of the* d*-Hamming neighborhood* $\Gamma^d\mathbf{A}$ *of any set* $\mathbf{A} \subset \mathbf{X}^n$, $|\mathbf{A}| = m$, *and* $d(\mathbf{A}) \geqslant 2$, *is at least*

$$\binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{n-2k+2-d} + \binom{1+a_{n-2k}}{n-2k-d+1}$$
$$+ \binom{1+a_{n-2k-1}}{n-2k-d} + \cdots + \binom{1+a_s}{s-d+1}$$

whenever $d \leqslant 1$ *and the coefficients* a_i*'s are uniquely determined by the* n*-matched representation* (10) *of* m.

We remark here that the minimum can be achieved by a certain pure-parity Hamming sphere $\mathbf{A}_0$, and that this minimum neighborhood size can be expressed as

$$|\Gamma^d \mathbf{A}_0| = G_{d-1}(m + \varphi(m, n), n).$$

Finally, we generalize the symmetric Frankl–Füredi theorem to sets with prescribed hole-diameter.

Theorem 4. *To any two subsets* $\mathbf{A}$ *and* $\mathbf{B}$ *of* $\mathbf{X}^n$ *satisfying* $d(\mathbf{A}) \leq 2$, $d(\mathbf{B}) \leq 2$, *there exist two pure-parity Hamming spheres* $\mathbf{A}_0$, *centered at* $\mathbf{0}$, *and* $\mathbf{B}_0$, *centered at* $\mathbf{1}$, *such that*

$$|\mathbf{A}_0| = |\mathbf{A}|, \quad |\mathbf{B}_0| = |\mathbf{B}|, \quad \textit{and} \quad d(\mathbf{A}_0, \mathbf{B}_0) \geq d(\mathbf{A}, \mathbf{B}).$$

In the case when we impose different bounds on the hole-diameter of $\mathbf{A}$ and $\mathbf{B}$, the situation becomes more complex. The basic problem is that that the 1-neighborhood $\Gamma\mathbf{A}$ of a pure-parity Hamming sphere $\mathbf{A}$ is not necessarily a Hamming sphere, for it may have two incomplete layers. Therefore, the symmetric result cannot be generalized without imposing some condition on the cardinalities of $\mathbf{A}$ and $\mathbf{B}$. To do so, let us consider, for any $m \leq 2^{n-1}$, both the odd- and even-parity Hamming spheres with m elements. To each of them we consider the smallest (ordinary) Hamming sphere with the same center in which it is contained. It is clear that the sizes of these ordinary Hamming spheres are the same for all odd- (even-) parity Hamming spheres. Denote the smaller of the two sizes by $C(m, n)$. We have:

Theorem 5. *To a pair of subsets* $\mathbf{A}$ *and* $\mathbf{B}$ *of* $\mathbf{X}^n$ *satisfying* $d(\mathbf{A}) \geq 2$, *there exist a pure-parity Hamming sphere,* $\mathbf{A}_0$, *and an ordinary Hamming sphere,* $\mathbf{B}_0$, *such that*

$$|\mathbf{A}_0| = |\mathbf{A}|, \quad |\mathbf{B}_0| = |\mathbf{A}|, \quad \textit{and} \quad d(\mathbf{A}_0, \mathbf{B}_0) \geq d(\mathbf{A}, \mathbf{B}) \tag{12}$$

if and only if $d := d(\mathbf{A}, \mathbf{B})$ *satisfies*

$$C(|\mathbf{A}|, n) + G_{d-1}(|\mathbf{B}|, n) \leq 2^n. \tag{13}$$

An interesting problem would be to generalize the previous results to cases where $d(\mathbf{A})$ or $d(\mathbf{B}) \geq 3$.

3. Proofs

Proof of Theorem 1. With this proof, we shall take advantage of the natural correspondence between binary n-vectors (or binary n-sequences) and subsets of $N = \{1, 2, \ldots, n\}$. Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be a binary n-vector, then the corresponding set is $A = \{i \in N : x_i = 1\}$. Therefore, within this proof, $\mathbf{A}$ and $\mathbf{B}$ are considered sets of subsets (e.g. A, B) of N, instead of sets of binary n-vectors. The

Hamming distance between n-vectors, $d(\mathbf{x},\mathbf{y})$, carries over to become symmetric difference of sets, $d(A,B)$. If an n-vector $\mathbf{x}$ corresponds to the subset A of N, then $wt(\mathbf{x})=|A|$. These conventions enable us to develop a Frankl–Füredi-type proof.

Consider all the pairs $\{(A,A^*): A\in\mathbf{A},\ A^*\notin\mathbf{A}, A^*$ has the same parity as members of $\mathbf{A}$, and $|A|<|A^*|\}$. If no such pair exists, then $\mathbf{A}$ is a pure-parity Hamming sphere centered at N (i.e. centered at the all-one vector), and we are done. Otherside, let us choose a pair $(\mathbf{A},A^*)$ with minimum Hamming distance $d(\mathbf{A},A^*)$. Assume this pair is (A_0,A_0^*). Note that $d(A_0,A_0^*)$ is a positive even number. Set

$$U=A_0-A_0^*,\quad V=A_0^*-A_0,\qquad |U|<|V|.$$

For the two sets U and V, define the following two operations (Up and Down):

$$\mathbf{U}(A)=\begin{cases}A-U+V, & \text{if } U\subset A,\ V\cap A=\emptyset,\ A-U+V\notin\mathbf{A},\\ A, & \text{otherwise}\end{cases}$$

$$\mathbf{D}(B)=\begin{cases}B-V+U, & \text{if } V\subset B,\ U\cap B=\emptyset,\ B-V+U\notin\mathbf{B},\\ B, & \text{otherwise}\end{cases}$$

It is clear that the mappings $\mathbf{U}$ and $\mathbf{D}$ are one-to-one and thus $|\mathbf{U}(\mathbf{A})|=|\mathbf{A}|$, $|\mathbf{D}(\mathbf{B})|=|\mathbf{B}|$, further $||\mathbf{U}(A)|\geqslant|A|$. Also note that, for every $A\in\mathbf{A}$, $\mathbf{U}(A)$ has the same parity as A. Since $\mathbf{U}(A_0)=A_0^*$, the application of $\mathbf{U}$ strictly increases the quantity $\sum_{A\in\mathbf{A}}|A|$. In the sequel, we will show that $d(\mathbf{U}(\mathbf{A}),\mathbf{D}(\mathbf{B}))\geqslant d(\mathbf{A},\mathbf{B})$, and thus the repeated joint applications of $\mathbf{U}$ and $\mathbf{D}$ finally lead to a pure-parity Hamming sphere $\mathbf{A}'$ having the same parity as $\mathbf{A}$, and an arbitrary set $\mathbf{B}'$ with the claimed properties.

Consider two subsets, $A\in\mathbf{A}$, $B\in\mathbf{B}$, and write $A':=\mathbf{U}(A)$, $B':=\mathbf{D}(B)$. If $A\in\mathbf{U}(\mathbf{A})\cap\mathbf{A}$ and $B\in\mathbf{D}(\mathbf{B})\cap\mathbf{B}$, then clearly $A'=A$, $B'=B$, and $d(A',B')\geqslant d(A,B)$. Similarly, if $A'\in\mathbf{U}(\mathbf{A})-\mathbf{A}$, $B'\in\mathbf{D}(\mathbf{B})-\mathbf{B}$, then $A'=A-U+V$, $B'=B-V+U$ and $d(A',B')=d(A,B)\geqslant d(\mathbf{A},\mathbf{B})$. This settles the cases of two old and two new sets.

If one set is new and the other unchanged, e.g.

$$A'=\mathbf{U}(A)\in\mathbf{U}(\mathbf{A})-\mathbf{A},\qquad B\in\mathbf{D}(\mathbf{B})\cap\mathbf{B},$$

then $A'=A-U+V$.

If $V\subset B$ and $U\cap B=\emptyset$, then B has not been changed to a smaller set by the operation $\mathbf{D}$ only because $\hat{B}=(B-V+U)\in\mathbf{B}$. Thus $d(A',B)=d(A,\hat{B})\geqslant d(\mathbf{A},\mathbf{B})$.

If the condition $(V\subset B, U\cap B=\emptyset)$ is not satisfied and $U=\emptyset$, then $V\not\subset B$. Further $A_0\subset A_0^*$ and A_0, A_0^* have the same parity, thus the minimality condition on (A_0,A_0^*) implies $|V|=2$. Let $V=\{\mathbf{v}_1,\mathbf{v}_2\}$. There are two cases, $V\cap B=\emptyset$ or $|V\cap B|=1$. In the former case we have

$$d(A',B)=d(A+V,B)=d(A,B)+|V|\geqslant d(\mathbf{A},\mathbf{B})+2.$$

In the latter case we have

$$d(A', B) = d(A + V, B) = d(A, B) \geq d(\mathbf{A}, \mathbf{B}).$$

Finally, if $1 \leq |U| < |V|$ and the condition ($V \subset B$, $U \cap B = \emptyset$) is not satisfied, then there are two elements $\mathbf{u} \in U$, $\mathbf{v} \in V$ such that at least one of the inclusions $\mathbf{v} \in V - B$, $\mathbf{u} \in U \cap B$ holds. Let $\hat{A} := A - (U - \mathbf{u}) + (V - \mathbf{v})$, then $|\hat{A}| = |A'| > |A|$ and $d(A, \hat{A}) < d(A_0, A_0^*)$. The definition of A_0 thus implies $\hat{A} \in \mathbf{A}$. Furthermore, we have $A' = \hat{A} - \mathbf{u} + \mathbf{v}$. If we delete the element $\mathbf{u}$ from $\hat{A}$, then $d(\hat{A}, B)$ increases by 1 if $\mathbf{u} \in B$ and decreases by 1 if $\mathbf{u} \notin B$. On the other hand if we adjoin the element $\mathbf{v}$ to $(\hat{A} - \mathbf{u})$ then $d(\hat{A} - \mathbf{u}, B)$ increases by 1 if $\mathbf{v} \notin B$ and decreases by 1 if $\mathbf{v} \in B$. Combining all situations, we obtain

$$d(A', B) = d(\hat{A} - \mathbf{u} + \mathbf{v}, B) \geq d(\hat{A}, B) \geq d(\mathbf{A}, \mathbf{B}). \quad \square$$

Proof of Lemma 1. We shall prove the uniqueness of the first representation only. The other case is similar. First, observe that

$$m' \leq \binom{n-1}{n-2k} + \binom{n-2}{n-2k-1} + \cdots + \binom{2k}{1} = \binom{n}{n-2k} - 1.$$

Going back to (10a), it is easy to convince oneself that there exists a unique k satisfying

$$\sum_{i=0}^{k-1} \binom{n}{n-2i} \leq m < \sum_{i=0}^{k} \binom{n}{n-2i}$$

provided that $m < 2^{n-1}$.

According to the Kruskal–Katona result (Lemma K in the first section of this paper), m' has an unique $(n-2k)$-canonical representation,

$$m' = \binom{a_{n-2k}}{n-2k} + \binom{a_{n-2k-1}}{n-2k-1} + \cdots + \binom{a_s}{s}$$

with $a_{n-2k} > a_{n-2k-1} > \cdots > a_s \geq s \geq 1$. Furthermore, we have $n > a_{n-2k}$ because

$$m' < \binom{n}{n-2k}.$$

Combining the above arguments, we have shown that m has a unique representation in the form (10). $\square$

Proof of Lemma 2. Invoking Pascal's identity on the first k binomial coefficients of the n-matched representation, (10), of m, we obtain

$$\begin{aligned} m = {} & \binom{n-1}{n-1} + \binom{n-1}{n-2} + \binom{n-1}{n-3} + \cdots + \binom{n-1}{n-2k+2} \\ & + \binom{n-1}{n-2k+1} + \binom{a_{n-2k}}{n-2k} + \binom{a_{n-2k-1}}{n-2k-1} + \cdots + \binom{a_s}{s} \end{aligned} \tag{14}$$

By definition, (14) is Katona's $(n-1)$-bounded representation of m.

Invoking Pascal's identity on the first l terms of the n-mismatched representation of m, i.e. (11), we obtain

$$m=\binom{n-1}{n-1}+\binom{n-1}{n-2}+\cdots+\binom{n-1}{n-2l+1}+\binom{n-1}{n-2l}$$
$$+\binom{b_{n-2l-1}}{n-2l-1}+\binom{b_{n-2l-2}}{n-2l-2}+\cdots+\binom{b_t}{t}. \tag{15}$$

Again, (15) is Katona's $(n-1)$-bounded representation of m. By Lemma HK in the first section, the $(n-1)$-bounded representation of m is unique. Therefore, (14) and (15) are identical.

Hence there are two possible cases. In one case we have

$$k=l,\quad s=t,\quad a_{n-2k}=n-1,$$
$$a_i=b_i,\quad \text{for } s\leqslant i\leqslant n-2k-1.$$

In the other case, we have

$$k=l+1,\quad s=t,\quad b_{n-2l-1}=n-1,$$
$$a_i=b_i\quad \text{for } s\leqslant i\leqslant n-2k.$$

In either case, we can invoke Pascal's identity and verify easily that $\varphi^*(m,n)=\varphi^{**}(m,n)$. $\square$

Proof of Lemma 3. Partition $\mathbf{A}_0$ into $(\mathbf{A}_{\text{odd}},\mathbf{A}_{\text{even}})$, where $\mathbf{A}_{\text{odd}}$ $(\mathbf{A}_{\text{even}})$ consists of odd- (even-) parity members of $\mathbf{A}_0$. We wish to show that either $\mathbf{A}_{\text{odd}}$ or $\mathbf{A}_{\text{even}}$ is empty.

Assume that neither $\mathbf{A}_{\text{odd}}$ nor $\mathbf{A}_{\text{even}}$ is empty and let $d(\mathbf{A}_{\text{odd}},\mathbf{A}_{\text{even}})=2a+1$. We have $a\geqslant 1$ because $d(\mathbf{A}_0)\geqslant 2$. There exist $\mathbf{x}_{\text{odd}}$ in $\mathbf{A}_{\text{odd}}$ and $\mathbf{x}_{\text{even}}$ in $\mathbf{A}_{\text{even}}$ such that the two vectors differ in only the bit positions $i_1,i_2,\ldots,i_{2a+1}$. Let $\mathbf{A}'_{\text{odd}}$ be obtained from $\mathbf{A}_{\text{odd}}$ by inverting the i_1th, i_2th, …, and i_{2a-1}th bits. Then $\mathbf{A}'_{\text{odd}}\cap\mathbf{A}_{\text{even}}=\emptyset$, $\mathbf{A}'_0=\mathbf{A}'_{\text{odd}}\cup\mathbf{A}_{\text{even}}$ has pure even-parity, $|\mathbf{A}'_0|=|\mathbf{A}_0|=m$, and $|\Gamma\mathbf{A}'_{\text{odd}}|=|\Gamma\mathbf{A}_{\text{odd}}|$. Let $\mathbf{x}^*$ be obtained from $\mathbf{x}_{\text{odd}}$ by inverting the i_1th, i_2th, …, and the i_{2a}th bits. Then $\mathbf{x}^*\in\Gamma\mathbf{A}'_{\text{odd}}\cap\Gamma\mathbf{A}_{\text{even}}$. Hence $|\Gamma\mathbf{A}'_0|<|\Gamma\mathbf{A}'_{\text{odd}}|+|\Gamma\mathbf{A}_{\text{even}}|=|\Gamma\mathbf{A}_{\text{odd}}|+|\Gamma\mathbf{A}_{\text{even}}|=|\Gamma\mathbf{A}_0|$. But $\mathbf{A}_0$ is assumed to have minimum outer boundary, hence the desired contradiction is obtained. $\square$

Proof of Theorem 2. For convenience assume that n is even. Also, let

$$m=\binom{n}{n}+\binom{n}{n-2}+\cdots+\binom{n}{n-2k+2}+m',$$
$$m'=\binom{a_{n-2k}}{n-2k}+\binom{a_{n-2k-1}}{n-2k-1}+\cdots+\binom{a_t}{t}$$

where $n>a_{n-2k}>a_{n-2k-1}>\cdots>a_t\geqslant t\geqslant 1$.

By Lemma 3, it suffices to show that

$$\varphi^*(m,n)=\min_{\substack{|\mathbf{A}|=m\\ \mathbf{A}\text{ even}}}|\Gamma\mathbf{A}-\mathbf{A}|.$$

Let $\mathbf{A}_0$ be the m-element subset of $\mathbf{X}^n$ which contains:

(1) all even-weight vectors of weight between $n-2k+2$ and n inclusively, and

(2) m' vectors of weight $n-2k$ chosen according to Kruskal's scheme.

Then we have

$$|\Gamma\mathbf{A}_0-\mathbf{A}_0|=\binom{n}{n-1}+\binom{n}{n-3}+\cdots+\binom{n}{n-2k+1}+F(m',n-2k)$$
$$=\varphi^*(m,n).$$

Therefore $\varphi^*(m,n)\geqslant\varphi(m,n)$.

On the other hand, let $\mathbf{A}_1$ be an m-element subset of $\mathbf{X}^n$ consisting of even vectors and have minimum boundary, i.e. $|\Gamma\mathbf{A}_1-\mathbf{A}_1|=\varphi(m,n)$. Let $\mathbf{B}_1:=\mathbf{X}^n-\Gamma\mathbf{A}_1$. Applying Theorem 1 to $\mathbf{A}_1$ and $\mathbf{B}_1$, we obtain an even-parity Hamming sphere $\mathbf{A}_2$ and a set $\mathbf{B}_2$ with $d(\mathbf{A}_2,\mathbf{B}_2)\geqslant d(\mathbf{A}_1,\mathbf{B}_1)=2$. Therefore, $\mathbf{B}_2\subset\mathbf{X}^n-\Gamma\mathbf{A}_2$ and $|\mathbf{B}_2|\leqslant 2^n-|\Gamma\mathbf{A}_2|\leqslant 2^n-|\Gamma\mathbf{A}_1|=|\mathbf{B}_1|$. By Theorem 1, $|\mathbf{A}_1|=|\mathbf{A}_2|$, $|\mathbf{B}_1|=|\mathbf{B}_2|$. Therefore $|\Gamma\mathbf{A}_2-\mathbf{A}_2|=\varphi(m,n)$, i.e. $\mathbf{A}_2$ also has minimum boundary. Comparing $\mathbf{A}_2$ to the corresponding $\mathbf{A}_0$ which has the same center and the same number of layers as $\mathbf{A}_2$ but the outermost layer is chosen according to the Kruskal–Katona scheme to minimize boundary, we have $|\Gamma\mathbf{A}_2|\geqslant|\Gamma\mathbf{A}_0|$, or $\varphi(m,n)\geqslant\varphi^*(m,n)$. □

Proof of Theorem 3. Let $\mathbf{A}_0$ be an even-parity Hamming sphere with the given size whose outermost layer is chosen according to the Kruskal–Katona scheme. Then we have

$$|\Gamma^d(\mathbf{A}_0)|=|\Gamma^{d-1}(\Gamma\mathbf{A}_0)|=G_{d-1}(|\Gamma\mathbf{A}_0|,n)$$
$$\leqslant G_{d-1}(|\Gamma\mathbf{A}|,n)\leqslant|\Gamma^d(\mathbf{A})|,$$

for any other m-element set $\mathbf{A}$. The first equality is obvious. The inequalities follow from Theorem 2, resp. Theorem KH. The second equality also becomes apparent after the following algebraic manipulations.

$$|\Gamma\mathbf{A}_0|=\binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{n-2k+1}+\binom{a_{n-2k}}{n-2k}$$
$$+\binom{a_{n-2k-1}}{n-2k-1}+\cdots+\binom{a_s}{s}$$
$$+\binom{a_{n-2k}}{n-2k-1}+\binom{a_{n-2k-1}}{n-2k-2}+\cdots+\binom{a_s}{s-1}$$
$$=\binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{n-2k+1}+\binom{1+a_{n-2k}}{n-2k}$$
$$+\binom{1+a_{n-2k-1}}{n-2k-1}+\cdots+\binom{1+a_s}{s}.$$

With $n \geqslant 1+a_{n-2k} > 1+a_{n-2k-1} > \cdots > 1+a_s > s \geqslant 1$, the above form is the unique n-bounded representation of $|\Gamma\mathbf{A}_0|$ promised by Lemma HK. Further since

$$
\begin{aligned}
|\Gamma^d(\mathbf{A}_0)= & \binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{n-2k+2-d}+\binom{a_{n-2k}}{n-2k-d+1} \\
& +\binom{a_{n-2k-1}}{n-2k-d}+\cdots+\binom{a_s}{s-d+1} \\
& +\binom{a_{n-2k}}{n-2k-d}+\binom{a_{n-2k-1}}{n-2k-1-d}+\cdots+\binom{a_s}{s-d} \\
= & \binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{n-2k+2-d} \\
& +\binom{1+a_{n-2k}}{n-2k-d+1}+\binom{1+a_{n-2k-1}}{n-2k-d}+\cdots+\binom{1+a_s}{s-d+1},
\end{aligned}
$$

we have, by definition,

$$|\Gamma^d(\mathbf{A}_0)| = G_{d-1}(|\Gamma\mathbf{A}_0|, n). \quad \square$$

Lemma 4. *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be pure-parity subsets of* $\mathbf{X}^n$. *There exist pure-parity Hamming spheres* $\mathbf{A}_0$ *and* $\mathbf{B}_0$, *centered at* $\mathbf{1}$ *and* $\mathbf{0}$ *respectively and having the same parity as* $\mathbf{A}$ *and* $\mathbf{B}$ *respectively such that* $|\mathbf{A}_0| = |\mathbf{A}|$, $|\mathbf{B}_0| = |\mathbf{B}|$, *and* $d(\mathbf{A}_0, \mathbf{B}_0) \geqslant d(\mathbf{A}, \mathbf{B})$.

Proof. Consider the set of pairs

$$\{(A, A^*): A \in \mathbf{A},\ A^* \notin \mathbf{A},\ |A| < |A^*|,\ A^* \text{ has the same parity as members of } \mathbf{A}\}$$

and

$$\{(B, B^*): B \in \mathbf{B},\ B^* \notin \mathbf{B},\ |B| > |B^*|,\ B^* \text{ has the same parity as members of } \mathbf{B}\}.$$

If there are no such pairs, then $\mathbf{A}$ is a $\mathbf{1}$-centered, and $\mathbf{B}$ a $\mathbf{0}$-centered, pure-parity Hamming sphere and we are done.

Otherwise, let us choose a pair (A, A^*) or (B, B^*) with minimum Hamming distance $d(A, A^*)$ or $d(B, B^*)$.

Without loss of generality, assume this minimum pair is (A_0, A_0^*). Then defining the two operations (Up and Down) as in the proof of Theorem 1, we can follow through the rest of Theorem 1 without any change. Thus this lemma is proved. $\square$

Proof of Theorem 4. As in the proof of Theorem 1, the natural correspondence between subsets of $N = \{1, 2, \ldots, n\}$ and binary n-vectors is used.

Let $d = d(\mathbf{A}, \mathbf{B})$. Partition $\mathbf{A}$ into $(\mathbf{A}_{\text{even}}, \mathbf{A}_{\text{odd}})$ and $\mathbf{B}$ into $(\mathbf{B}_{\text{even}}, \mathbf{B}_{\text{odd}})$, where $\mathbf{A}_{\text{even}}$, $\mathbf{B}_{\text{even}}$ consist of even-parity vectors and $\mathbf{A}_{\text{odd}}$, $\mathbf{B}_{\text{odd}}$ of odd-parity vectors. Assume first that d is even. We have $d(\mathbf{A}_{\text{even}}, \mathbf{B}_{\text{even}})$, $d(\mathbf{A}_{\text{odd}}, \mathbf{B}_{\text{odd}}) \geqslant d$,

$d(\mathbf{A}_{\text{even}}, \mathbf{B}_{\text{odd}})$, $d(\mathbf{A}_{\text{odd}}, \mathbf{B}_{\text{even}}) \geq d+1$. Let $\mathbf{A}'_{\text{odd}}$ be obtained from $\mathbf{A}_{\text{odd}}$ by inverting the first bit in every vector, and let $\mathbf{B}'_{\text{odd}}$ be obtained similarly from $\mathbf{B}_{\text{odd}}$. Then we have

$$d(\mathbf{A}'_{\text{odd}}, \mathbf{B}'_{\text{odd}}),\ d(\mathbf{A}_{\text{even}}, \mathbf{B}'_{\text{odd}}),\ d(\mathbf{A}'_{\text{odd}}, \mathbf{B}_{\text{even}}) \geq d.$$

We also have $\mathbf{A}_{\text{even}} \cap \mathbf{A}'_{\text{odd}} = \emptyset$, $\mathbf{B}_{\text{even}} \cap \mathbf{B}'_{\text{odd}} = \emptyset$ because $d(\mathbf{A})$, $d(\mathbf{B}) \geq 2$. Let $\mathbf{A}' = \mathbf{A}_{\text{even}} \cup \mathbf{A}'_{\text{odd}}$, $\mathbf{B}' = \mathbf{B}_{\text{even}} \cup \mathbf{B}'_{\text{odd}}$. Then $\mathbf{A}'$ and $\mathbf{B}'$ are both pure parity sets and

$$|\mathbf{A}'| = |\mathbf{A}|, \quad |\mathbf{B}'| = |\mathbf{B}|, \quad d(\mathbf{A}', \mathbf{B}') \geq d.$$

Now we use Lemma 4 on $\mathbf{A}'$ and $\mathbf{B}'$ to complete the proof. The case when d is odd can be proved similarly. □

In order to prove the last theorem, we need yet another technical result:

Lemma 5. *$C(m, n)$ is the minimum cardinality of an ordinary Hamming sphere that contains a pure-parity Hamming sphere of m elements.*

Proof. Let $\mathbf{A}$ be any m-element pure-parity Hamming sphere, and let $\mathbf{S}$ be the smallest (ordinary) Hamming sphere containing $\mathbf{A}$. We propose to show that there exists some pure-parity Hamming sphere $\hat{\mathbf{A}}$ with the same center as $\mathbf{S}$, such that $\mathbf{A} \subset \hat{\mathbf{A}} \subset \mathbf{S}$. This implies the lemma.

Without loss of generality, assume $\mathbf{A}$ odd-parity. Let the center of $\mathbf{A}$ be $\mathbf{c}$ and that of $\mathbf{S}$ be $\mathbf{0}$. Let $w = wt(\mathbf{c})$, and let the vectors on the outmost layer of $\mathbf{S}$ have weight k. If w is even, then let $\hat{\mathbf{A}}$ consist of all vectors of weight $1, 3, \ldots, k$ in $\mathbf{S}$. If w is odd, then let $\hat{\mathbf{A}}$ consist of all vectors of weight $0, 2, \ldots, k$ in $\mathbf{S}$. In either case, $\hat{\mathbf{A}}$ is a pure-parity Hamming sphere centered at $\mathbf{0}$ satisfying $\mathbf{A} \subset \hat{\mathbf{A}} \subset \mathbf{S}$. □

Finally, we provide a

Proof of Theorem 5. Let $\mathbf{A}$ be a pure-parity Hamming sphere centered at $\mathbf{1}$ with its outermost layer chosen according to the Kruskal–Katona scheme (i.e. choose the vectors with the lowest possible lexicographic orders). The parity of $\mathbf{A}$ is chosen so that its minimum containing Hamming sphere, which has cardinality $C(|\mathbf{A}|, n)$, is also centered at $\mathbf{1}$. Let $\mathbf{B}$ be a Hamming sphere centered at $\mathbf{0}$ whose outermost layer contains vectors with the highest possible lexicographic order. If $|\mathbf{A}|$ and $|\mathbf{B}|$ satisfy (13), then $d(\mathbf{A}, \mathbf{B})$ satisfies (12).

To prove the converse implication, suppose that there exist a Hamming sphere $\mathbf{B}_0$ and a pure-parity Hamming sphere $\mathbf{A}_0$ satisfying (12). By Theorem KH,

$$|\Gamma^{d-1}\mathbf{B}_0| \geq G_{d-1}(|\mathbf{B}_0|, n).$$

Further by Lemma 5,

$$|\mathbf{X}^n - \Gamma^{d-1}\mathbf{B}_0| \geq C(|\mathbf{A}_0|, n).$$

Combining the two inequalities, we obtain the theorem. □

Appendix A. Another proof of Theorem 2

This proof takes resemblance to Katona's proof of Harper's Theorem. In particular, Eckhoff–Wegner's Lemma (Lemma EW in this text) is used. The proof goes by induction based on a recursive inequality for $\varphi^*(m, n)$. We shall repeatedly consider two arbitrary integers, $m_0>0$, $m_1>0$, along with the expansions (cf. Lemma 1):

$$m_0=\binom{n-1}{n-1}+\binom{n-1}{n-3}+\cdots+\binom{n-1}{n-2l+1}+m_0',$$

$$m_1=\binom{n-1}{n-2}+\binom{n-1}{n-4}+\cdots+\binom{n-1}{n-2k+2}+m_1'$$

where

$$m_0'=\binom{a_{n-2l-1}}{n-2l-1}+\binom{a_{n-2l-2}}{n-2l-2}+\cdots+\binom{a_s}{s},$$

$$m_1'=\binom{b_{n-2k}}{n-2k}+\binom{b_{n-2k-1}}{n-2k-1}+\cdots+\binom{b_t}{t}$$

with

$$n-1>a_{n-2l-1}>a_{n-2l-2}>\cdots>a_s\geqslant s\geqslant 1,$$

$$n-1>b_{n-2k}>b_{n-2k-1}>\cdots>b_t\geqslant t\geqslant 1.$$

Note that m_0-m_0' has l terms, m_1-m_1' has $k-1$ terms, and

$$m_0'<\binom{n-1}{n-2l-1} \quad\text{and}\quad m_1'<\binom{n-1}{n-2k}.$$

Lemma A1: *If $k=l$ or $k=l+1$, then we have*

$$\varphi^*(m_0+m_1, n)\leqslant\max[m_0; \varphi^*(m_1, n-1)]+\max[m_1; \varphi^*(m_0, n-1)].$$

Proof. If $k=l$, then we have

$$m_0+m_1=\binom{n}{n}+\binom{n}{n-2}+\cdots+\binom{n}{n-2k+2}+m_0'+m_1'$$

where $m_0'+m_1'<\binom{n}{n-2k}$. Therefore we have

$$\varphi^*(m_0+m_1, n)=\binom{n}{n-1}+\binom{n}{n-3}+\cdots+\binom{n}{n-2k+1}$$
$$+F(m_0'+m_1', n-2k).$$

Lemma EW implies $F(m_0'+m_1', n-2k) \leq \max[m_0'; F(m_1', n-2k)] + F(m_0', n-2k-1)$. Thus

$$\begin{aligned}
&\varphi^*(m_0+m_1, n)\\
&\quad\leq \binom{n-1}{n-1}+\binom{n-1}{n-3}+\cdots+\binom{n-1}{n-2k+1}+\max[m_0'; F(m_1', n-2k)]\\
&\qquad+\binom{n-1}{n-2}+\binom{n-1}{n-4}+\cdots+\binom{n-1}{n-2k}+F(m_0', n-2k-1)\\
&\quad=\max[m_0; \varphi^*(m_1, n-1)]+\varphi^*(m_0, n-1),
\end{aligned}$$

implying the lemma. □

The case $k=l+1$ is similar.

Lemma A2: *$\varphi^*(m, n)$ is non-decreasing in m.*

Proof. Straightforward. □

Lemma A3:

$$\varphi^*(m_0+m_1, n) \leq \max[m_0; \varphi^*(m_1, n-1)] + \max[m_1; \varphi^*(m_0, n-1)].$$

Proof. If $k=l$ or $l+1$, we are done by Lemma A1. If $k>l+1$, we have $\varphi^*(m_1, n-1) \geq m_0$ and $m_1 \geq \varphi^*(m_0, n-1)$. Let

$$m_2=\binom{n-1}{n-1}+\binom{n-1}{n-3}+\cdots+\binom{n-1}{n-2k+3}>m_0.$$

Note that $\varphi^*(m_1, n-1) \geq m_2$ and $m_1 \geq \varphi^*(m_2, n-1)$. By Lemma A1 we have

$$\begin{aligned}
\varphi^*(m_2+m_1, n) &\leq \max[m_2; \varphi^*(m_1, n-1)]+\max[m_1; \varphi^*(m_2, n-1)]\\
&=\varphi^*(m_1, n-1)+m_1.
\end{aligned}$$

By Lemma A2 we have

$$\begin{aligned}
\varphi^*(m_0+m_1, n) &\leq \varphi^*(m_2+m_1, n)\\
&\leq \varphi^*(m_1, n-1)+m_1\\
&\leq \max[m_0; \varphi^*(m_1, n-1)]+\max[m_1; \varphi^*(m_0, n-1)].
\end{aligned}$$

The case $k<l$ is similar. □

Lemma A4. *For any m, $0 \leq m \leq 2^{n-1}$, there exist nonnegative m_0 and m_1, $m_0+m_1=m$ such that*

$$\varphi(m, n) \geq \max[m_0; \varphi(m_1, n-1)]+\max[m_1; \varphi(m_0, n-1)].$$

Proof. Let $\mathbf{A}$, $|\mathbf{A}|=m$, have minimum boundary, i.e. $|\Gamma\mathbf{A}-\mathbf{A}|=\varphi(m, n)$. Partition

$\mathbf{A}$ into $\mathbf{A}_0$ and $\mathbf{A}_1$ where members of $\mathbf{A}_0$ have their first bit zero and members of $\mathbf{A}_1$ have first bit 1. Similarly, partition $\Gamma\mathbf{A}-\mathbf{A}$ into $\mathbf{B}_0$ and $\mathbf{B}_1$. Let $m_0=|\mathbf{A}_0|$, $m_1=|\mathbf{A}_1|$, then $m_0+m_1=m$.

Let us introduce some notations. Let $\mathbf{x}'$ denote the $(n-1)$-vector obtained from the n-vector $\mathbf{x}$ by deleting the first bit. Let $\mathbf{A}_0'$, $\mathbf{A}_1'$, $\mathbf{B}_0'$, $\mathbf{B}_1'$ be obtained by deleting the first bit of every vector in $\mathbf{A}_0$, $\mathbf{A}_1$, $\mathbf{B}_0$, $\mathbf{B}_1$, respectively. Note that $|\mathbf{A}_0'|=|\mathbf{A}_0|$, $|\mathbf{A}_1'|=|\mathbf{A}_1|$, $|\mathbf{B}_0'|=|\mathbf{B}_0|$, $|\mathbf{B}_1'|=|\mathbf{B}_1|$, and $\mathbf{A}_0, \mathbf{A}_1, \mathbf{B}_0, \mathbf{B}_1\subset\{0,1\}^n$, $\mathbf{A}_0', \mathbf{A}_1', \mathbf{B}_0', \mathbf{B}_1'\subset\{0,1\}^{n-1}$.

For any $4\mathbf{y}'\in\Gamma\mathbf{A}_0'-\mathbf{A}_0'$, we have $\mathbf{y}'\in\mathbf{B}_0'$ and $\Gamma\mathbf{A}_0'-\mathbf{A}_0'\subset\mathbf{B}_0'$. From this we have $|\mathbf{B}_0'|\geqslant|\Gamma\mathbf{A}_0'-\mathbf{A}_0'|\geqslant\varphi(m_0,n-1)$. For any $\mathbf{x}'\in\mathbf{A}_1'$, we have $\mathbf{x}'\in\mathbf{B}_0'$, and $\mathbf{A}_1'\subset\mathbf{B}_0'$. Hence $|\mathbf{B}_0'|\geqslant|\mathbf{A}_1'|=m_1$. Therefore, we have

$$|\mathbf{B}_0'|\geqslant\max[m_1;\ \varphi(m_0,n-1)].$$

Similarly, we have

$$|\mathbf{B}_1'|\geqslant\max[m_0;\ \varphi(m_1,n-1)].$$

Since $\varphi(m,n)=|\Gamma\mathbf{A}-\mathbf{A}|=|\mathbf{B}_0|+|\mathbf{B}_1|=|\mathbf{A}_0'|+|\mathbf{B}_1'|$, we have proved the lemma. $\square$

Proof of Theorem 2. The inequality $\varphi(m,n)\leqslant\varphi^*(m,n)$ is straightforward. We shall prove $\varphi(m,n)\geqslant\varphi^*(m,n)$ by induction on n.

The case $n=1$ is trivial. Assume $\varphi(m,i)=\varphi^*(m,i)$ for all $i<n$. Combining Lemmas 3 and 4, we have

$$\varphi^*(m,n)\leqslant\varphi(m,n).\quad\square$$

Appendix B

In this appendix, we present an m-element set which has minimum boundary $G(m,n)$ but is not a Hamming sphere. Assume

$$m=\binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{p'}+m'$$

where

$$m'=\binom{a_{p'-1}}{p'-1}+\binom{a_{p'-2}}{p'-2}+\cdots+\binom{a_{r'}}{r'}$$

with $n>a_{p'-1}>a_{p'-2}>\cdots>a_{r'}\geqslant r'\geqslant1$. Further, assume $a_{p'-1}<n-1$ and $a_i>i>1$. Let $m'=m''+m'''$ where

$$m''=\binom{a_{p'-1}-1}{p'-1}+\binom{a_{p'-2}-1}{p'-2}+\cdots+\binom{a_{r'-1}}{r'},\tag{B1}$$

$$m'''=\binom{a_{p'-1}-1}{p'-2}+\binom{a_{p'-2}-1}{p'-3}+\cdots+\binom{a_{r'}-1}{r'-1}.\tag{B2}$$

Note that $a_{p'-1}-1>a_{p'-2}-1>\cdots>a_{r'}-1\geq r'$ and $r'-1\geq 1$, so (B1) is the $(p'-1)$-canonical representation of m'' and (B2) the $(p'-2)$-canonical representation of m'''. Also note that $F(m'',p'-1)=m'''$.

Let $\mathbf{A}$ be the m-element set consisting of the following:

(1) $\mathbf{A}_1$: all binary n-vectors of weight $\geq p'$,

(2) $\mathbf{A}_2$: m' n-vectors of weight $p'-1$ which have the m' lowest lexicographic order (i.e., m' vectors chosen according to the Kruskal–Katona scheme), and

(3) $\mathbf{A}_3$: all direct descandants of $\mathbf{A}_2$ (i.e. all $(p'-2)$-weight vectors obtainable from $\mathbf{A}_2$ by substituting a 1 with a 0). It is easy to show that

$$\begin{aligned}|\Gamma^d\mathbf{A}| &= \binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{p'-d}\\ &\quad+\binom{a_{p'-1}-1}{p'-d-1}+\binom{a_{p'-2}-1}{p'-d-2}+\cdots+\binom{a_{r'}-1}{r'-d}\\ &\quad+\binom{a_{p'-1}-1}{p'-d-2}+\binom{a_{p'-2}-1}{p'-d-3}+\cdots+\binom{a_{r'}-1}{r'-d-1}\\ &= \binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{p'-d}\\ &\quad+\binom{a_{p'-1}}{p'-d-1}+\binom{a_{p'-2}}{p'-d-2}+\cdots+\binom{a_{r'}}{r'-d}\\ &= G_d(m,n).\end{aligned}$$

Hence $\mathbf{A}$ has minimum boundary.

On the other hand, $\mathbf{A}$ is not a Hamming sphere. To see this, suppose $\mathbf{A}$ is a Hamming sphere. Then $\mathbf{A}$ must consist of $n-p'+1$ complete layers and m' elements on the $(n-p'+2)$-th layer from its center. (The center itself is considered the first layer.) Consider the possible poisition of the center $\mathbf{x}_0$. It is not $\mathbf{1}$ for then $\mathbf{A}$ would not be a Hamming sphere. And if $wt(\mathbf{x}_0)\leq n-2$, then there exists some $\mathbf{y}$, $wt(\mathbf{y})=p'$, such that $d(\mathbf{x}_0,\mathbf{y})\geq n-p'+2$ and $\mathbf{A}$ would not be a Hamming sphere. This leaves the last possibility that $wt(\mathbf{x}_0)=n-1$. But in this case, there are $\binom{n-1}{p'-1}$ vectors of weight p' which are at distance $n'-p+1$ from $\mathbf{x}_0$. Since $m'<\binom{n-1}{p'-1}$ as assumed earlier, $wt(\mathbf{x}_0)\neq n-1$. Therefore, $\mathbf{A}$ is not a Hamming sphere.

References

[1] R. Ahlswede, P. Gacs and J. Körner, Bounds on conditional probabilities with applications in multi-user communication, Z. Wahrscheinlichkeitstheorie verw. Geb. 34 (1976) 157–177; Correction to ..., ibid 39 (1977) 353–354.

[2] L.A. Bassalygo, V.A. Zinovev, V.V. Zablov, M.S. Pinsker and A.S. Poltyrev, Bounds for codes with unequal protection of two message sets (in Russian) Probl. Per. Inf. 15 (3) (1979) 40–49.

[3] I. Csiszár and J. Körner, Information Theory: Coding Theorems for Discrete Memoryless Systems (Academic Press, New York, 1981) and (Akadémiai Kiadó, Budapest, 1981).

[4] J. Eckhoff and G. Wegner, Über einen Satz von Kruskal, Periodica Math. Hung. 6 (1975) 137–142.
[5] P. Frankl and Z. Füredi, A short proof of a theorem of Harper about Hamming-spheres, Discrete Math. 39 (1981) 311–313.
[6] K.H. Harper, Optimal numberings and isoperimetric problems on graphs, J. Combinatorial Theory 1 (1966) 385–393
[7] G. Katona: A theorem of finite sets, in: Theory of Graphs, Proc. Colloq. Tihany, 1966 (Akadémiai Kiadó, Budapest 1968) 187–207.
[8] G.O.H. Katona, The Hamming sphere has minimum boundary, Studia Sci. Math. Hungar. 10 (1977) 131–140.
[9] J.B. Kruskal, The numbers of simplices in a complex, in: Math. Opt. Techniques (Univ. of California Press, 1963) 251–278.
[10] G.A. Margulis, Probabilistic characteristics of graphs with large connectivity, Problems of Information Transmission 10 (1974) 174–179.
[11] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam–New York, 1977).
[12] R.L. McEliece, E.R. Rodemich, H.C. Rumsey and L.R. Welch, New upper bounds on the rate of a code via the Delsarte–MacWilliams identities, IEEE Trans. Inform. Theory 23 (1977) 157–166.