

On Some Properties of Intersection and Union of Spheres in Hamming Metric

Haykaz E. Danoyan

Yerevan State University
e-mail: hdanoyan@yandex.ru

Abstract

The problems of intersection and union of spheres of the same radius in Hamming metric are considered. The formula for number of points in intersection is derived in case of two spheres. It is proved that three or more spheres of radius R_C (covering radius of a code C) centered at points belonging to some quasi-perfect code C intersect at most at one point. It is also proved that the increase of cardinality of union of spheres of the same radius, depending on radius, is a concave function and can have at most one or two maximum values depending on length.

Keywords: Nearest neighbors, best-match, Hamming spheres, concave function, quasi-perfect code.

1. Introduction

Let $E = \{0; 1\}$. Denote by E^n the set of vertices of the unit cube, that is each vector can be represented as $\alpha = (\alpha_1, \dots, \alpha_n)$, where $\alpha_i \in E$, $i = 1, \dots, n$. For each pair of vectors α, β denote by $d(\alpha, \beta)$ the Hamming distance between the vectors α and β . For $\alpha \in E^n$ denote by $S_r^n(\alpha)$ the sphere with centre α and radius r , that is $S_r^n(\alpha) = \{\beta \in E^n, d(\alpha, \beta) \leq r\}$. The carrier of the vector $\alpha \in E^n$ we define as $car(\alpha) = \{i/\alpha_i \neq 0, i = 1, \dots, n\}$. Denote by $w(\alpha)$ the weight of vector α , that is $w(\alpha) = |car(\alpha)|$. Denote by N_n the set of the first n natural numbers, i.e. $N_n = \{1, \dots, n\}$. A code C will be called a subset of E^n [1]. Usually the codes are considered for which some other additional properties take place such as linearity, cyclicity, etc. In some cases a problem to find the intersection of k spheres of the fixed radius can arise [2-4]. We will consider this problem for a simple case, namely when the centers of the spheres belong to a quasi-perfect code with the covering radius R . Recall that a code C is called quasi perfect [1] if the following condition holds: $R_c = r_c + 1$, where $R_c = \max_{x \in E^n} \min_{c \in C} d(x, c)$ and $r_c = \lfloor (d_c - 1)/2 \rfloor$. The number d_c is called a minimum distance of the code C , i.e. $d_c = \min_{c_1, c_2 \in C, c_1 \neq c_2} d(c_1, c_2)$. We also consider the problem of increase of union of spheres of some radius depending on the radius. More precisely let us have a set $C \subseteq E^n$ and let $f_C(r) = |\bigcup_{\alpha \in C} S_r^n(\alpha) - \bigcup_{\alpha \in C} S_{r-1}^n(\alpha)|$. It is important to check [2],[5] if the function $f_C(r)$ is concave, with one or two maximal values depending on n and C .

2. Intersection of Two Spheres

In the next section we will consider the problem of intersection of $k(k > 2)$ spheres in some cases, so it is useful at first to consider the case of two spheres. Suppose we have two spheres with centers α and β and radii r_1 and r_2 respectively. We denote the intersection of the mentioned spheres by $I_{r_1, r_2}^n(\alpha, \beta)$ i.e. $I_{r_1, r_2}^n(\alpha, \beta) = S_{r_1}^n(\alpha) \cap S_{r_2}^n(\beta)$. It is easy to show that each case can be reduced to the case when $\alpha = 0$, therefore furthermore we assume that the mentioned case takes place. Without losing generality we assume, that $r_2 \leq r_1$. It is easy to see that when $r_1 + r_2 < d$ (where $d = d(\alpha, \beta)$) the considered intersection is empty, so we suppose that $r_1 + r_2 \geq d$. We denote the cardinality of intersection by $I_{r_1, r_2}^n(d)$. Let us take any vector γ and find out conditions, under which the vector γ belongs to the set $I_{r_1, r_2}^n(\alpha, \beta)$. Let $car(\gamma) \cap car(\beta) = y$ and $car(\gamma) \setminus car(\beta) = x$ (Figure 1).

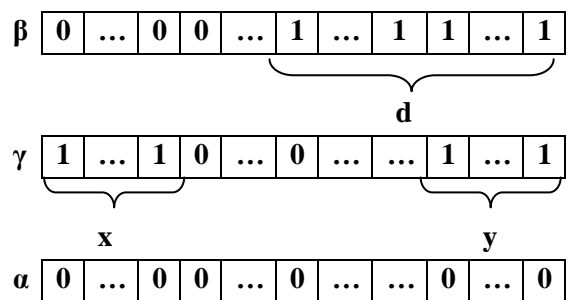


Fig. 1.

In order for γ belongs to the intersection, x and y should satisfy the following system of inequalities:

$$\begin{cases} x + y \leq r_1 \\ d - x + y \leq r_2. \end{cases}$$

Let us denote $a = \lfloor \frac{r_1 - r_2 + d}{2} \rfloor$. Consider the following three cases.

Case a. $0 < r_1 \leq d$. It is easy to see, that when $x \leq a$ then $r_1 - x \geq r_2 - d + x$ and when $x > a$, then $r_1 - x < r_2 - d + x$ (Fig. 2).

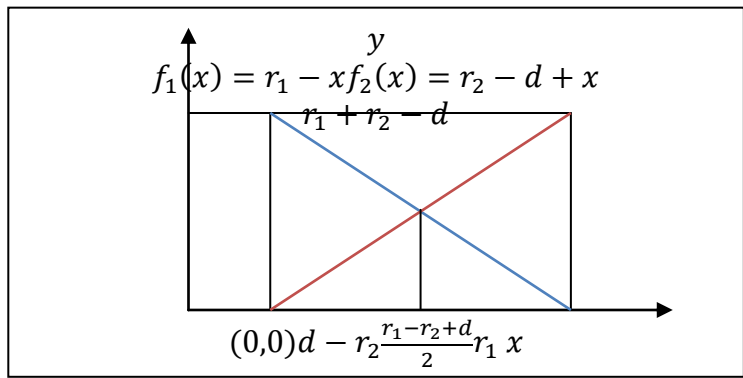


Fig. 2.

Therefore

$$I_{r_1 r_2}^n(d) = \sum_{i=d-r_2}^a \sum_{j=0}^{r_2-d+i} \binom{d}{i} \binom{n-d}{j} + \sum_{i=a+1}^{r_1} \sum_{j=0}^{r_1-i} \binom{d}{i} \binom{n-d}{j}.$$

In case when $r_1 + r_2 = d$ we can write (3) in a simpler form:

$$I_{r_1 r_2}^n(d) = \binom{r_1 + r_2}{r_1}.$$

Case b. $0 < r_2 \leq d, d < r_1 < n$. This case, in its turn, is divided into two separate cases:

Subcase b.1. $r_2 \geq r_1 - d$. By straightforward verification we get that when $x \leq a$ then $r_1 - x \geq r_2 - d + x$ and when $x > a$ then $r_1 - x < r_2 - d + x$ (Fig. 3).

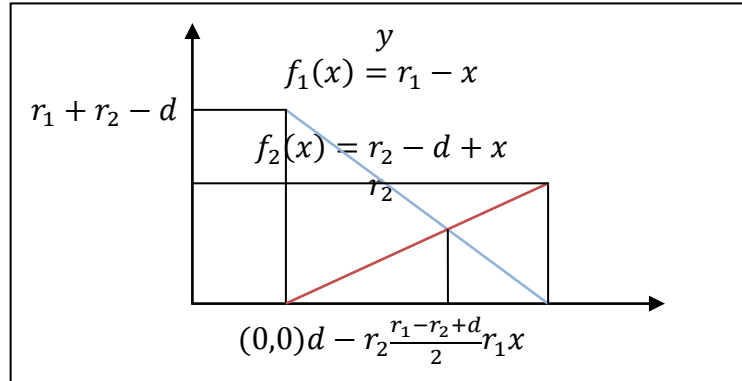


Fig. 3.

Therefore

$$I_{r_1 r_2}^n(d) = \sum_{i=d-r_2}^a \sum_{j=0}^{r_2-d+i} \binom{d}{i} \binom{n-d}{j} + \sum_{i=a+1}^d \sum_{j=0}^{r_1-i} \binom{d}{i} \binom{n-d}{j}.$$

Subcase b.2. $r_2 < r_1 - d$. In this case we get that $r_1 - x \geq r_2 - m + x$ when $d - r_2 \leq x \leq d$.

Therefore

$$I_{r_1 r_2}^n(d) = \sum_{i=d-r_2}^d \sum_{j=0}^{r_2-d+i} \binom{d}{i} \binom{n-d}{j}.$$

Case c. $d < r_2 \leq r_1 \leq n$. This case is also divided into two separate cases.

Subcase c.1. $r_1 > r_2 + d$. We get that when $x \leq a$ then $r_1 - x \geq r_2 - d + x$ and when $x > a$ then $r_1 - x < r_2 - d + x$ (Fig. 4).

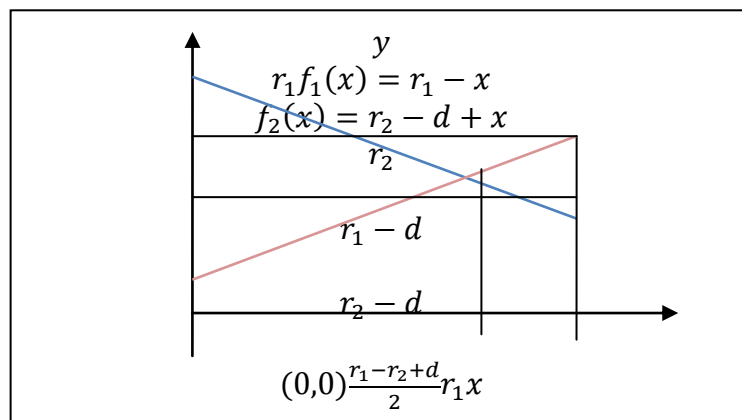


Fig. 4.

Therefore

$$I_{r_1 r_2}^d(d) = \sum_{i=0}^a \sum_{j=0}^{r_2-d+i} \binom{d}{i} \binom{n-d}{j} + \sum_{i=a+1}^d \sum_{j=0}^{r_1-i} \binom{d}{i} \binom{n-d}{j}.$$

Subcase c. $2.r_1 \leq r_2 + d$. In this case we get that $r_1 - x \geq r_2 - d + x$ when $d - r_2 \leq x \leq d$.

Therefore

$$I_{r_1 r_2}^n(d) = \sum_{i=0}^d \sum_{j=0}^{r_2-d+i} \binom{d}{i} \binom{n-d}{j}.$$

3. Intersection of Spheres Centered at Codewords of Quasi-perfect Code

Suppose we have spheres with radii r_1, r_2, \dots, r_k centered at points a_1, a_2, \dots, a_k respectively. Now we consider the intersection of k ($k \geq 3$) spheres with the radius R in case when the centers of spheres are codewords of any quasi-perfect code. As we mentioned, we can assume that $a_1 = 0$.

Proposition 1. Let vectors a_1, \dots, a_k be codewords of the quasi-perfect code with an even minimum distance $d = 2t$ ($t \geq 2$), then $|\bigcap_{i=1}^k S_R^n(a_i)| = 1$ if and only if

I. $d(a_i, a_j) = 2t, i \neq j,$

II. $\bigcap_{i=2}^k \text{car}(a_i) = t.$

Otherwise, the considered intersection is empty.

Proof. Necessity is obvious let us prove the sufficiency. Note that in this case we have $R = t, r = t - 1$. From the condition $d = 2t$ it follows that the intersection of the spheres of radius R centered at the points a_1, \dots, a_k is nonempty only if $d(a_i, a_j) = 2t, i \neq j$. So we get $w(a_2) = \dots = w(a_k) = 2t$ and $|\text{car}(a_i) \cap \text{car}(a_j)| = t, i, j = 2, \dots, k, i \neq j$. Let $z \in I_R^n(0, a_i)$. From the reasoning of the previous section it follows that $w(z) = t, \text{car}(z) \subseteq \text{car}(a_i)$ and $\text{car}(z) \subseteq \text{car}(a_j)$ therefore there is only z belonging to the intersection.

Now let us have vectors a_1, \dots, a_k which are codewords of any quasi-perfect code with an odd minimum distance, i.e. $d_c = 2t - 1$. This means that the covering radius of the code is $R_c = t$. Suppose we want to know the intersection of spheres with the radius t centered at a_1, \dots, a_k . As we mentioned, consider that $a_1 = 0$. Partition the set $\{2, \dots, k\}$ into two nonintersecting subsets K_1 and K_2 in the following way

$$i \in \begin{cases} K_1 & \text{if } w(a_i) = 2t - 1 \\ K_2 & \text{if } w(a_i) = 2t \end{cases}.$$

From the condition $d_c = 2t - 1$ follows that the considered intersection is not empty only when $|K_1| \leq 1$. Without losing generality assume that $K_1 = \{1\}$. Let Now we can formulate the following:

Proposition 2. Let vectors a_1, \dots, a_k be codewords of the quasi-perfect code with an odd minimum distance $d = 2t - 1$ ($t \geq 2$), then $|\bigcap_{i=1}^k S_R^n(a_i)| = 1$ if and only if

I. $d(a_i, a_j) = 2t, d(a_1, a_j) = 2t - 1$

II. $\bigcap_{i=2}^k \text{car}(a_i) = t.$

Otherwise the considered intersection is empty.

Proof. The schema of proof is analogous to proposition 1.

4. Variation Function of Area Size of Sphere System is Concave

Consider an arbitrary $\alpha \in E^n$. Then it is easy to check that for a fixed n the function $f_\alpha(r) = |S_r^n(\alpha) - S_{r-1}^n(\alpha)|$ is concave. For n odd there are two maximums of $f_\alpha(r)$ at $(n-1)/2$ and

$(n + 1)/2$. When n is even, then there is one maximal value at the point $n/2$. In a generalized model a number of packed spheres can be considered. Given a subset $C \subseteq E^n$ and let $f_C(r) = |\cup_{\alpha \in C} S_r^n(\alpha) - \cup_{\alpha \in C} S_{r-1}^n(\alpha)|$. It is important to check if the function $f_C(r)$ is also concave, with one or two maximal values depending on n and C . A harder generalization will be the case of different radii but our interest will be restricted to the basic case of one fixed r . There can also be considered not the spheres but the spherical structures [6].

Consider the case of two vertices, α and β . If one of these vectors is the negation of the other, then: if n is odd, there is one maximum at $(n - 1)/2$ and $f_C(r) = 0$ for $r > (n - 1)/2$; when n is even, then $f_{\{\alpha,\beta\}}(r)$ is increasing in interval $r < n/2$ and $f_{\{\alpha,\beta\}}(r) = 0$ when $r > n/2$. It reminds to compare the following 2 values: $f_{\{\alpha,\beta\}}(n/2 - 1) = 2 \binom{n}{n/2 - 1}$ and $f_{\{\alpha,\beta\}}(n/2) = \binom{n}{n/2}$. It is easy to check that the only maximum accepts at $n/2 - 1$, just it needs to take into account that n is even.

Now consider the case of α and β , not opposite in E^n . Choose an index i and the variable x_i so that $\alpha_i = \beta_i$. Partition E^n in the direction i , then α and β belong to one of the parts of E^n , let it be the sub-cube $E_{x_i=0}^{n-1}$. Denote by α^i and β^i the projections of α and β to $E_{x_i=0}^{n-1}$. The areas of our consideration n , $S_r^n(\alpha) \cup S_r^n(\beta)$ and $S_r^n(\alpha) \cup S_r^n(\beta) - S_{r-1}^n(\alpha) \cup S_{r-1}^n(\beta)$, can be partitioned in the direction i . In these two $n - 1$ dimensional sub-cubes we receive the same pair of vertices: α' and β' , and the radius r in $E_{x_i=0}^{n-1}$, and α'' and β'' and the radius $r - 1$ in $E_{x_i=1}^{n-1}$. In these terms $f_{\{\alpha,\beta\}}(r) = f_{\{\alpha',\beta'\}}(r) + f_{\{\alpha'',\beta''\}}(r - 1)$. In fact, we have the same function and the same points for E^{n-1} . If suppose that f is concave, having 1 or 2 maximal values, then this shifted sum will have the same properties.

Now we consider the general case of arbitrary $C \subseteq E^n$. Denote by $C'_{x_i=0}$ and $C'_{x_i=1}$ the partition compounds of C in direction x_i . Let $C''_{x_i=0}$ and $C''_{x_i=1}$ be projections of $C'_{x_i=0}$ and $C'_{x_i=1}$ in direction x_i . In the first step, when $r = 1$ we receive: in $E_{x_i=1}^{n-1}$ a union of $\cup_{\alpha \in C_{x_i=1}} S_1^n(\alpha)$ and $C''_{x_i=0}$, and similarly in $E_{x_i=0}^{n-1}$ a union of $\cup_{\alpha \in C_{x_i=0}} S_1^n(\alpha)$ and $C''_{x_i=1}$. In reality, in dimension $n - 1$ we have to consider two sets of vertices – those are basic in that cube and these vertices draw r spheres around, and the projection vertices that draw $r - 1$ spheres around. The second set may add some new neighbours to the basic set produced by the first set. The difficulty to watch these sets concerns the radii difference. To use the induction hypotheses we have to transform the constructions so that a situation appears, that is standard in dimension $n - 1$. For this purpose by an evident note it is sufficient to consider not the basic sets of vertices but the ones appeared after the first step $-(\cup_{\alpha \in C_{x_i=1}} S_1^n(\alpha)) \cup C''_{x_i=0}$ in $E_{x_i=1}^{n-1}$ and $(\cup_{\alpha \in C_{x_i=0}} S_1^n(\alpha)) \cup C''_{x_i=1}$ in $E_{x_i=0}^{n-1}$. In this case the basic f will appear as the sum of 2 functions in dimension $n - 1$ by the radius $r - 1$.

At this stage we have 2 concave functions in $n - 1$, which have 1 or 2 maximums by the supposition of induction. It is evident that the sum of functions will increase when functions increase separately, and that it decreases in part in case of decrease in both of them. Consider the point ξ of the first decrease in f . At least one of the sub-functions has its decrease at ξ . Let this be the function at $E_{x_i=1}^{n-1}$. The sensitive part that initiates this decrease will be the set $C'_{x_i=1}$. The complementary part can't be sensitive because its radius is higher in $E_{x_i=0}^{n-1}$ and its decrease must happen earlier and this will cause the summary decrease *inf*. Then, the projection of $C'_{x_i=1}$ that appears with the radius $r - 1$ in $E_{x_i=0}^{n-1}$ will have the same size in the next step when the radius is equal to r . This will sufficiently initiate the decrease in the sub-function at $E_{x_i=0}^{n-1}$.

References

- [1] F. J. Mac Williams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 1977.
- [2] I. Honkala, “On the intersection and unions of Hamming Spheres”, *The Very Knowledge of Coding*, pp. 70-81, 1987.
- [3] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, *Covering Codes*, 1997.
- [4] R.L. Rivest, “On the optimality of Elias's algorithm for performing best-match searches”, *Information Processing*, pp. 678-681, 1974.
- [5] Yu.Zhuravlev, *Selected Scientific Works*, (in russian), 1998.
- [6] L. Aslanyan, “Metric decompositions and the discrete isoperimetry”, *IFAC Symposium on Manufacturing, Modelling, Management and Control*, pp. 433-438, 2000.

Submitted 24.12.2012, accepted 18.02.2013.

Հեմինգի մետրիկայում սֆերաների հատման և միավորման որոշ հատկությունների մասին

Հ. Դանոյան

Ամփոփում

Դիտարկվում է Հեմինգի մետրիկայում սֆերաների հատման և միավորման կետերի գտնելու խնդիրը: Բերված է բանաձև՝ երկու տարբեր շառավիղներով սֆերաների հատման համար: Ապացուցված է, որ երեք և ավելի r շառավիղով սֆերաները, որոնց զազաթները պատկանում են որևէ քվադրատային կոդի, կարող են հատվել ամենաշատը մեկ կետով (R -ը նշված կոդի ծածկման շառավիղն է): Ապացուցված է նաև, որ սֆերաների միավորման շառավիղից կախված ֆունկցիայի աճը ունի մեկ կամ երկու մաքսիմում՝ կախված տարածության չափողականությունից:

О некоторых свойствах пересечения и объединения сфер в метрике Хемминга

А. Даноян

Аннотация

Рассматривается проблема нахождения пересечения и объединения сфер в метрике Хемминга. Приведена формула для числа точек пересечения для двух сфер. Доказано, что три и более сферы радиуса R , центры которых принадлежат некоторому квазисовершенному коду C , могут пересекаться лишь в одной точке (R радиус покрытия кода C). Также доказано, что возрастание функции числа точек в объединении некоторых сфер от радиуса может иметь один или два максимума в зависимости от меры пространства.