Reconstruction of the support of an object from the support of its autocorrelation

J. R. Fienup, T. R. Crimmins, and W. Holsztynski*

Radar and Optics Division, Environmental Research Institute of Michigan, P.O. Box 8618, Ann Arbor, Michigan 48107

Received July 23, 1981

The phase-retrieval problem consists of the reconstruction of an object from the modulus of its Fourier transform or, equivalently, from its autocorrelation. This paper describes a number of results relating to the reconstruction of the support of an object from the support of its autocorrelation. Methods for reconstructing the object's support are given for objects whose support is convex and for certain objects consisting of collections of distinct points. The uniqueness of solutions is discussed. In addition, for the objects consisting of collections of points, a simple method is shown for completely reconstructing the object functions.

1. INTRODUCTION

In astronomy, x-ray crystallography, and other disciplines one often wishes to reconstruct an object from its autocorrelation or, equivalently, from the modulus of its Fourier transform (i.e., the phase-retrieval problem).[1] It is also useful to be able to reconstruct just the support of the object (the set of points over which it is nonzero). In some cases, for example, to find the relative locations of a collection of pointlike stars, the object's support is the desired information. In addition, once the object's support is known, the reconstruction of the object by the iterative method[2] is simplified. Therefore we are motivated to find a quick way to determine the support of the object from the support of its autocorrelation.

In the general case there may be many solutions for the object's support, given the autocorrelation support. In the following sections, a method for generating sets containing all possible solutions is given. In addition, for the special case of convex sets a method for generating a family of support solutions is described. For the special case of objects consisting of sets of discrete points, this method is shown to yield a unique support solution unless the vector separations of the points in the object satisfy certain redundancy types of conditions. If, instead of manipulating the autocorrelation support, one uses the autocorrelation function, then for the same objects one can reconstruct the object itself.

2. DEFINITIONS AND BACKGROUND

The results shown in this paper apply to functions on Euclidean spaces of any number of dimensions except where otherwise noted. For simplicity we consider only objects represented by real, nonnegative functions, $f(x) \geq 0$, where $x \in E^N$ (N-dimensional Euclidian space). The *support* S of a nonnegative function $f(x)$ is the smallest closed set such that the integral of $f(x)$ over the complement of S in E^N is zero. [Roughly speaking, S is the set on which $f(x) > 0$.] In this paper we consider only functions with compact (i.e., closed and bounded) support. If $f(x)$ is a finite positive linear combination of translates of the delta function, then S is a *finite set*.

We will be making use of linear operations on sets. Let X and Y be subsets of E^N. Then the addition of two sets and multiplication by scalars is defined by

$$aX + bY \equiv \{ax + by{:}x \in X \text{ and } y \in Y\}, \tag{1a}$$

where a and b are real numbers. Similarly, the addition of a point (which can be thought of as a vector) $x \in E^N$ to a set is defined by

$$ax + bY \equiv \{ax + by{:}y \in Y\}, \tag{1b}$$

where again a and b are real numbers. Whereas these linear operations on sets enjoy some of the properties expected from addition and from multiplication by a scalar, other properties do not hold. For example, for a real number a and for sets X, Y, and Z, $(X + Y) + Z = X + (Y + Z)$; $a(bX) = (ab)X$; and $a(X + Y) = aX + aY$. However, $(a + b)X$ does not equal $aX + bX$ except for special cases. The role of zero in this case is played by the set of $\{0\}$ consisting of the single point $0 = (0, \ldots, 0) \in E^N$. We have $X + \{0\} = X$ and $a\{0\} = \{0\}$. But $X - X$ does not equal $\{0\}$ unless X consists of a single point. The *autocorrelation of* $f(x)$ is[3]

$$f \star f(x) = \int_{E^N} f(y)f(y + x)\mathrm{d}y \tag{2a}$$

$$= \int_{E^N} f(y)f(y - x)\mathrm{d}y. \tag{2b}$$

The autocorrelation of $f(x)$ is equal to the inverse Fourier transform of the squared modulus of the Fourier transform of $f(x)$. Note that the autocorrelation is (centro-) symmetric: $f \star f(-x) = f \star f(x)$. It is most illuminating to interpret Eq. (2a) as a weighted sum of translated versions of $f(x)$. That is, in the integrand of Eq. (2a), $f(y)$ acts as the weighting factor for $f(y + x)$, which is $f(x)$ translated by $-y$. If the support S of a nonnegative integrable function $f(x)$ is compact and if A is the support of its autocorrelation function $f \star f(x)$, then

$$\begin{aligned} A &= \bigcup_{y \in S} (S - y) \\ &= S - S = \{x - y{:}x, y \in S\}. \end{aligned} \tag{3}$$

0030-3941/82/050610-15$01.00

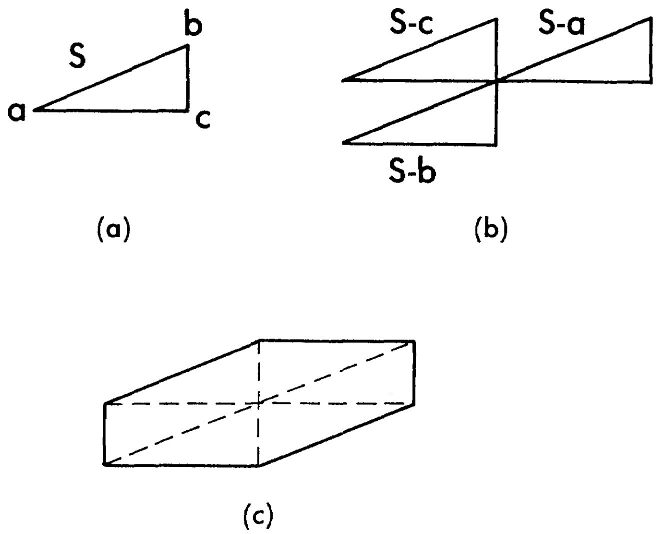

Fig. 1. (a) Set S, (b) three of the translates of S that make up A, (c) autocorrelation support $A = S - S$.

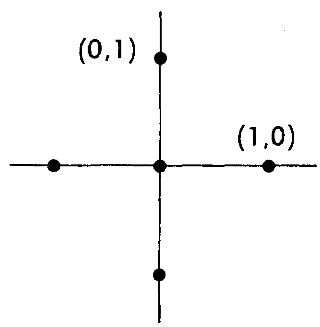

Fig. 2. A symmetric set that is not an autocorrelation support.

The proof of Eq. (3) is in Appendix A. Note that A is *symmetric*:

$$-A = A, \tag{4}$$

where $-A = \{-x{:}x \in A\}$. In addition,

$$0 \in A \tag{5}$$

as long as S is nonempty. To illustrate the interpretation of an autocorrelation support, consider the case of the two-dimensional support S shown in Fig. 1(a), having the form of a triangle with vertices at points a, b, and c. The autocorrelation support A can be thought of as being formed by successively translating S so that each point in S is at the origin and by taking the union of all these translates of S. Figure 1(b) shows three such translates, $(S - a)$, $(S - b)$, and $(S - c)$. The rest of A is filled in, as shown in Fig. 1(c), by including all $(S - y)$ such that $y \in S$.

We are concerned with the following problem. Given a symmetric set $A \subseteq E^N$, find sets $S \subseteq E^N$ that satisfy $A = S - S$.

Sets S_1 and S_2, which are subsets of E^N, are *equivalent*,

$$S_1 \sim S_2, \tag{6a}$$

if there exists a vector $v \in E^N$ such that

$$S_2 = v + \beta S_1 = \{v + \beta x{:}x \in S_1\}, \tag{6b}$$

where $\beta = +1$ or $\beta = -1$. From Eq. (3) it is easily seen that if S_1 is a solution to $S - S = A$, and if $S_2 \sim S_1$, then S_2 is also a solution. If S_1 is a solution and all other solutions are equivalent to S_1, then the solution is said to be *unique* and A is said to be *unambiguous*; if there exist any nonequivalent solutions, then the solutions is *nonunique* and A is *ambiguous*. For example, in one dimension the set of points $A = \{-1, 0, 1\}$ is unambiguous, having the unique solution $S = \{0, 1\}$; whereas the set of points $A = \{-3, -2, -1, 0, 1, 2, 3\}$ is ambiguous, having nonequivalent solutions $S_1 = \{0, 1, 3\}$ and $S_2 = \{0, 1, 2, 3\}$.

Not all symmetric sets that contain 0 are necessarily autocorrelation supports, as the following example shows. As shown in Fig. 2, let $A = \{(0, 0), (1, 0), (-1, 0), (0, 1), (0, -1)\}$. Because of the point (1, 0), a solution must include two points separated by (1, 0). Similarly, because of the point (0, 1), a solution must include two points separated by (0, 1). Therefore the solution must have at least three distinct noncollinear points. Of the three possible pairings of the three points, one has a separation along (1, 0), a second has a separation along (0, 1), and the third pair of points must have a separation vector that is not on the horizontal or vertical axes. However, all points in A are on the horizontal or vertical axes, and therefore there is no solution for $A = S - S$ in this case.

A set X is *convex* if for all $x, y \in X$,

$$tx + (1 - t)y \in X \tag{7}$$

for all $t \in [0, 1]$ (that is, if all points on the line segment between x and y are contained in X). The *convex hull* of a set X, denoted by c.hull(X), is given by the smallest convex subset of E^N containing X. Thus X is convex if and only if X = c.hull(X). If S is convex, then $A = S - S$ is also convex. More generally,

$$\text{c.hull}(X - X) = \text{c.hull}(X) - \text{c.hull}(X). \tag{8}$$

3. LOCATOR SETS

In many cases A is ambiguous, and so it would be useful to define a set that contains all possible solutions to the equation $A = S - S$. A set $L \subseteq E^N$ is defined as a *locator set* for A if for every closed set $S \subseteq E^N$ satisfying $A = S - S$, some translate of S is a subset of L, i.e., there exists a vector v such that

$$v + S \subseteq L. \tag{9}$$

There are many ways to generate locator sets. For example, for $v \in S$, $S - v \subseteq S - S = A$, and so A itself is a locator set. The smaller the locator set, the more tightly it bounds the possible solutions and the more informative it is. Consequently, we wish to find locator sets that are as small as possible. A smaller locator set than A is

$$L = A \cap H, \tag{10}$$

where H is any closed half-space of E^N with the origin on its boundary. To see this, choose $v \in S$ such that $S - v \subseteq H$. Then since $S - v \subseteq A$, it follows that $S - v \subseteq L = A \cap H$. A locator set that is often still smaller can be shown to be

$$L = \tfrac{1}{2}P, \tag{11}$$

where P is any N-dimensional parallelepiped (in two dimensions: parallelogram) containing A.

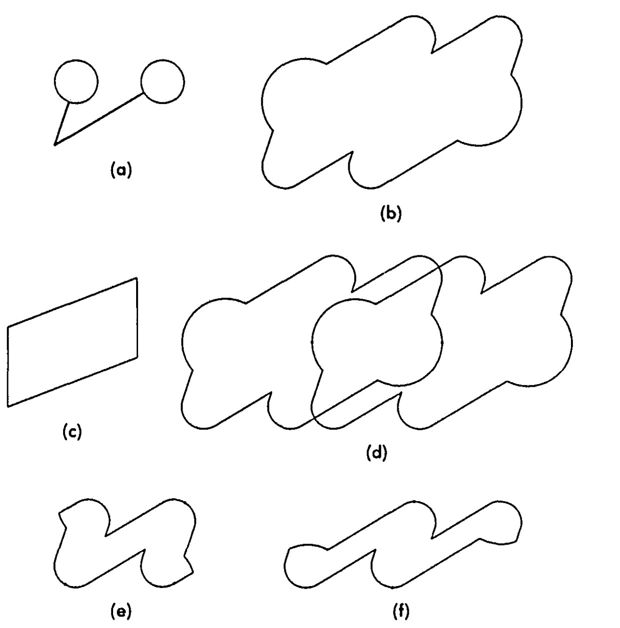

Fig. 3. Locator sets. (a) Set S, (b) $A = S - S$, (c) locator set $L = \frac{1}{2}P$, (d) formation of $L = A \cap (w + A)$, (e) and (f) two other members of the family of locator sets.

A particularly interesting locator set is given by the following intersection of two autocorrelation supports. If $w \in A$, then

$$L = A \cap (w + A) \tag{12}$$

is a locator set for A. Note that L is symmetric about the point $w/2$. The proof that this is a locator set is as follows: Suppose that S satisfies $A = S - S$. Since $w \in A$, there exist $u, v \in S$ such that $w = u - v$. Consider $z \in S - v$. Then $z = s - v$, where $s \in S, z = s - v \in A$, and $z = s - u + (u - v) = s - u + w \in A + w$. Therefore $z \in A \cap (A + w) = L$, and therefore $S - v \in L$.

Naturally, the most interesting (smallest) locator sets generated by this method of intersecting two autocorrelation supports are obtained by choosing w to be on the boundary of A. By choosing different points $w \in A$, a whole family of locator sets can be generated by this method.

The locator set defined by Eq. (12) can be shown to be a special case of the following more general locator set. Let W be a set contained in some $S' \sim S$ for every set S satisfying $S - S = A$. That is, W is an intersection of translates of all possible solutions. Then

$$L = \bigcap_{w \in W} (w + A) \tag{13}$$

is a locator set for A. The proof is as follows: Suppose that $S - S = A$ and $S \sim S'$ with $W \subseteq S'$. Then $S' - p \subseteq A$ for every $p \in S'$. Hence

$$S' \subseteq \bigcap_{p \in S'} (p + A) \subseteq \bigcap_{p \in W} (p + A). \tag{14}$$

Although Eq. (13) has the potential for producing particularly small locator sets, its practicality is limited by the fact that W is defined by all possible solutions to $S - S = A$, but that is what is assumed to be unknown. Nevertheless, one can make some use of Eq. (13). For example, if $S - S = A$ and $w \in A$, then there exists a translate S' of S such that $w \in S'$ and $0 \in S'$. Hence we can use $W = (0, w)$, which reduces Eq. (13) to Eq. (12).

Example 1

Consider the set S shown in Fig. 3(a), which consists of two balls joined by two thin rods, and its autocorrelation support $A = S - S$, shown in Fig. 3(b). An example of a locator set $\frac{1}{2}P$ is shown in Fig. 3(c); it is suggestive of the approximate size of S but not of any of the details of the shape of S. Figure 3(d) shows the generation of the locator set $L = A \cap (w + A)$ for a particular point $w \in A$. Figures 3(e) and 3(f) show two other members of this family of locator sets generated with two other points $w \in A$. These locator sets generated by intersecting two autocorrelation supports are suggestive of the shape of the solution (or solutions). This is especially true if one realizes that any solution must be contained within some translate of each of these locator sets. Unfortunately, for the general case, it is difficult to narrow down the solution any further: a way to combine the information from two or more of the family of locator sets has not been devised for the general case. However, as will be shown in the sections that follow, for special classes of sets much more can be done.

Example 2

Consider the set A consisting of a circle of radius 1. Figures 4(a)–4(c) show the locator sets $A \cap H$, $\frac{1}{2}P$, and $A \cap (w + A)$, respectively. In addition, Fig. 4(d) shows still another locator set for A, a circle of radius $1/\sqrt{3}$, which is due to Jung's theorem.[4] The areas of the four locator sets are $\pi/2 \simeq 1.571$ for the half circle, 1.000 for the square (parallelogram) with sides of length 1, $2\pi/3 - \sqrt{3/2} \simeq 1.228$ for the intersection of two circles, and $\pi/3 \simeq 1.047$ for the circle of radius $1/\sqrt{3}$. Consequently, $\frac{1}{2}P$ has the smallest area of the locator sets considered in this case. In other cases, such as in Example 1 above, $A \cap (w + A)$ may have a smaller area than $\frac{1}{2}P$. For example, the locator set shown in Fig. 3(e) has a smaller area than the locator set shown in Fig. 3(c). Furthermore, as was

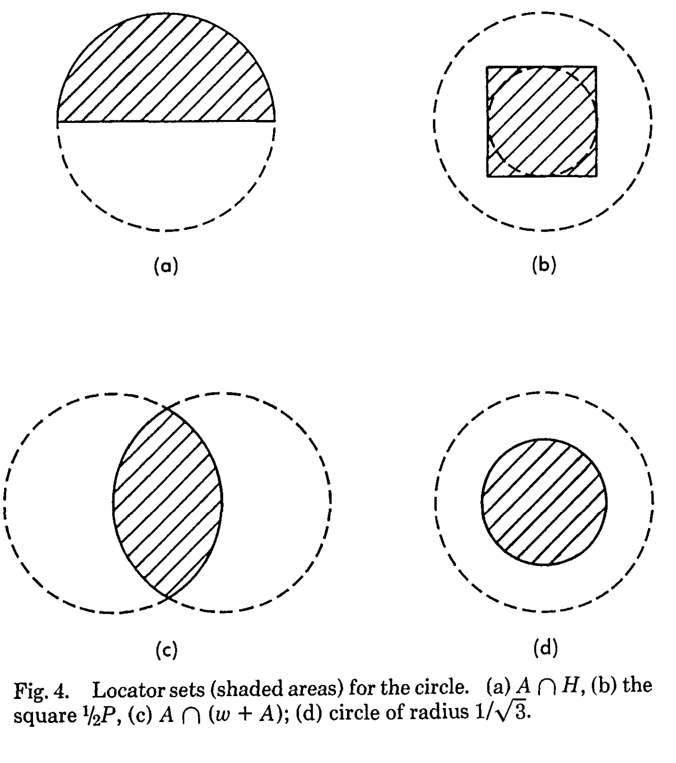

Fig. 4. Locator sets (shaded areas) for the circle. (a) $A \cap H$, (b) the square $\frac{1}{2}P$, (c) $A \cap (w + A)$; (d) circle of radius $1/\sqrt{3}$.

mentioned earlier, locators of the form $A \cap (w + A)$ tend to be more suggestive of the shape of the possible solutions.

4. CONVEX SETS

A number of interesting results hold for objects having convex support. In the following, statements are made about the uniqueness of convex solutions to $A = S - S$ for convex sets A, and methods of determining solutions are given.

All convex symmetric sets A have at least one solution

$$S = \tfrac{1}{2}A = \{x/2 : x \in A\}. \tag{15}$$

The proof is as follows: Let $u, v \in \tfrac{1}{2}A$. Then $2u \in A$, $2v \in A$, and $-2v \in A$. Therefore $u - v = \tfrac{1}{2}(2u) + \tfrac{1}{2}(-2v) \in A$, since A is convex, and so $(\tfrac{1}{2}A) - (\tfrac{1}{2}A) \subseteq A$. Now let $v \in A$. Then $v/2 \in \tfrac{1}{2}A$ and $-v/2 \in \tfrac{1}{2}A$. Therefore $v = (v/2) - (-v/2) \in (\tfrac{1}{2}A) - (\tfrac{1}{2}A)$, and so $A \subseteq (\tfrac{1}{2}A) - (\tfrac{1}{2}A)$. Therefore, for convex A,

$$A = (\tfrac{1}{2}A) - (\tfrac{1}{2}A). \tag{16}$$

For the one-dimensional convex case the result is trivial: the autocorrelation support A is just a line segment, and a unique solution is given by $S = \tfrac{1}{2}A$, which is just a segment of the line half of the length of the line segment A. An equivalent result for the one-dimensional convex case is the solution

$$S = A \cap (w + A), \tag{17}$$

where w is on the boundary of A (at one end of line segment A), or, in symbols, $w \in \partial(A)$.

4A. Autocorrelation Tri-Intersection for Convex Sets

For the two-dimensional convex case, we have the following result: Let $A \subseteq E^2$ be a closed convex symmetric set ($-A = A$) with nonnull interior, and let

$$w_1 \in \partial(A), \qquad w_2 \in \partial(A) \cap \partial(w_1 + A). \tag{18}$$

Furthermore, let

$$B = A \cap (w_1 + A) \cap (w_2 + A). \tag{19}$$

Then B is a solution to $A = S - S$, that is,

$$A = B - B. \tag{20}$$

The proof of this result is in Appendix B. Since w_1 can be any point on the boundary of A, Eq. (19) results in a family of solutions.

Example 3

Consider the set S shown in Fig. 5(a), which is the convex hull of the set shown in Fig. 3(a). Its autocorrelation support $A = S - S$ [which is the convex hull of Fig. 3(b)] is shown in Fig. 5(b). The parallelogram shown in Fig. 3(c) is a locator set for A. A member of the family of locator sets $A \cap (w + A)$ is shown by the intersection of A and $w + A$ in Fig. 5(c). A member of the family of solutions B is shown by the intersection of the three sets $A \cap (w_1 + A) \cap (w_2 + A)$ in Fig. 5(d). Two other examples of B obtained by using different points w_1 and w_2 are shown in Figs. 5(e) and 5(f).

4B. Three-Dimensional Intersections of Convex Sets

For convex sets, since in one dimension the intersection of two sets [Eq. (17)] results in the solution, and since in two dimensions the intersection of three sets [Eq. (19)] results in solutions, one might hope that in three dimensions the set

$$C = A \cap (w_1 + A) \cap (w_2 + A) \cap (w_3 + A) \tag{21}$$

would be a solution to $S - S = A$, where $w_1 \in \partial(A)$, $w_2 \in \partial(A) \cap \partial(w_1 + A)$, and $w_3 \in \partial(A) \cap \partial(w_1 + A) \cap \partial(w_2 + A)$. Unfortunately, this is generally not the case.

A counterexample to $C - C = A$ is the following: Consider S equal to a sphere of diameter 1, then $A = S - S$ is a sphere of radius 1 centered at the origin. Figures 6(a) and 6(b) show planar cuts through the centers of S and A, respectively. Figure 6(c) shows a planar cut through $A \cap (w_1 + A) \cap (w_2 + A)$ through the three points, 0, w_1, and w_2. $A \cap (w_1 + A) \cap (w_2 + A)$ has two vertices, one in front of the plane of the page and one behind the plane of the page, both at distance 1 from the center of each of the three intersecting spheres. Taking the intersection of this with $(w_3 + A)$, which is centered at one of the two vertices, gives us C, which is similar to a regular tetrahedron (it has the same vertices) but having spherical surfaces of radius 1 and centers at the opposite vertices in place of the four plane faces of a tetrahedron. Looking for a moment at the tetrahedron T having the same vertices as C (i.e., the convex hull of points 0, w_1, w_2 and w_3 having edges of length 1), we see that $T - T$ is a cuboctahedron, which has eight triangular faces and six square faces. Since $T \subseteq C$, then $T - T \subseteq C - C$. The surfaces of $C - C$ can be subdivided into 14 patches associated with the 14 faces of the cuboctahedron. It can be shown that the eight patches associated with the triangular faces coincide exactly with the surface of the sphere A of radius 1. However, the six patches corresponding to the square faces do not. For example, the

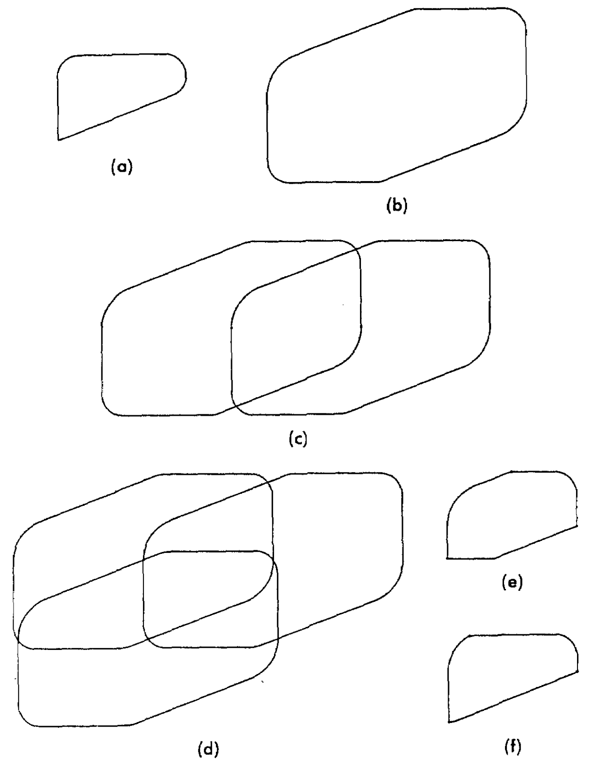

Fig. 5. Autocorrelation tri-intersection solution for convex sets. (a) Set S, (b) $A = S - S$, (c) formation of locator set $L = A \cap (w + A)$, (d) formation of solution $B = A \cap (w_1 + A) \cap (w_2 + A)$, (e) and (f) two other solutions of the form B.

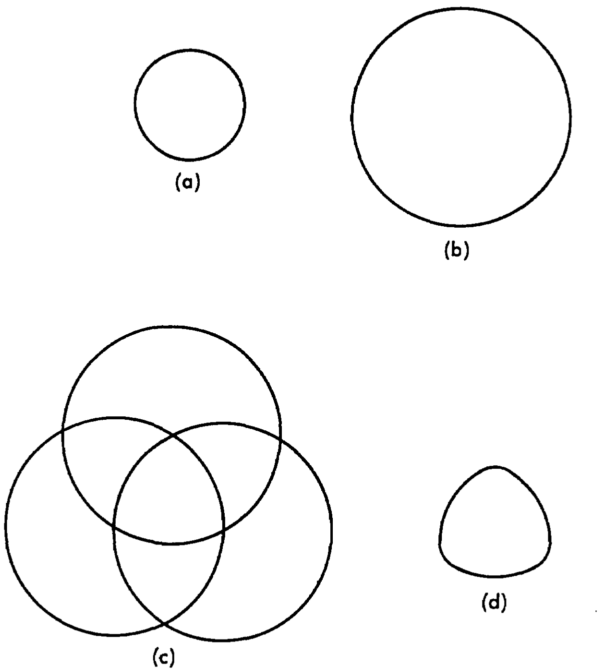

Fig. 6. Sphere/circle example. (a) Set S, (b) $A = S - S$, (c) $B = A \cap (w_1 + A) \cap (w_2 + A)$, (d) another solution for the circle combining the solutions (a) and (c).

distance from the origin to the center of each of those six patches is equal to the distance between the centers of two nonadjacent edges of C. This distance can be shown to be $\sqrt{3} - \sqrt{2}/2 \simeq 1.0249$. That is, the radius of $C - C$ is greater than that of the sphere A by about 2.49% at those points. Hence $C - C \neq A$.

4C. Linear Combinations of Convex Solutions

Returning to the N-dimensional case, if S_1 and S_2 are solutions to convex $A = S - S$, then

$$S_t = tS_1 + (1 - t)S_2 \tag{22}$$

is also a solution for $0 \leq t \leq 1$. The proof of this result is as follows:

$$\begin{aligned} S_t - S_t &= [tS_1 + (1 - t)S_2] - [tS_1 + (1 - t)S_2] \\ &= tS_1 - tS_1 + (1 - t)S_2 - (1 - t)S_2 \\ &= tA + (1 - t)A \\ &= A, \end{aligned} \tag{23}$$

since A is convex.

If S_1 is a solution, then so is $-S_1$. Then by using $t = 1/2$ and $S_2 = -S_1$ in Eq. (22), it is seen that

$$S_{1/2} = 1/2 S_1 - 1/2 S_1 = 1/2 A \tag{24}$$

is a solution, as was shown previously by Eq. (16).

Equation (22) can easily be generalized as follows: If $S_1, \ldots, S_n$ are solutions for convex A, and if $t_1, \ldots, t_n \geq 0$ and $t_1 + t_2 + \ldots + t_n = 1$, then

$$S = \sum_{i=1}^{n} t_i S_i \tag{25}$$

is also a solution.

In the two-dimensional case, if B_1 and B_2 are solutions obtained from the tri-intersection method of Eq. (19), then $tB_1 + (1 - t)B_2$ is a solution that usually cannot be generated by the tri-intersection method. Thus new solutions can be obtained by this method.

Example 4

Consider the two-dimensional convex set S shown in Fig. 6(a), consisting of a circle of diameter 1. $A = S - S$, consisting of a circle of radius 1, is shown in Fig. 6(b), and a tri-intersection solution B is shown as the intersection of three circles in Fig. 6(c). This solution is analogous to an equilateral triangle but having arcs of circles of radius 1 with centers at the opposite vertices for each of the three sides. It can easily be seen that all other solutions B generated by Eq. (19) are similar to the one shown in Fig. 6(c) except that they are rotated in the plane. The circle of diameter 1 shown in Fig. 6(a) is not of this form, but it is also a solution to A. As is shown by Eq. (24), $S = 1/2 A$ in Fig. 6(a) can be generated by applying Eq. (22) and by using $S_1 = -S_2 = B$ and $t = 1/2$. One of a family of additional solutions generated by Eq. (22) is shown in Fig. 6(d). It was generated by using $S_1 = 1/2 A$ in Fig. 6(a), $S_2 = B$ in Fig. 6(c), and $t = 1/2$.

4D. Ambiguity of Convex Sets

We now consider the question of uniqueness of convex solutions of $A = S - S$ for convex A. As was mentioned earlier, $S = 1/2 A$ is a solution. If all convex solutions are equivalent to $1/2 A$, then A is said to be *convex-unambiguous*. It was shown that in two dimensions one can generate a family of solutions by Eq. (19), the member of the family being determined by the choice of w_1. Equation (22) or Eq. (25) can then be used to generate still more solutions. Therefore one would suppose that convex sets A are generally convex-ambiguous. However, it is also possible that all solutions generated by Eq. (19) are equivalent, in which case A would be convex-unambiguous.

In what follows it is shown that in two dimensions if A is a parallelogram then A is convex-unambiguous. Let A be a parallelogram having vertices $w_1, -w_1, w_2$, and $-w_2$. By Eq. (12) a locator set for A is $L = A \cap (w_1 + A)$ since $w_1 \in A$. It is easily seen that $L = 1/2 w_1 + 1/2 A$, and so $L' = 1/2 A$, which has vertices $1/2 w_1, -1/2 w_1, 1/2 w_2, -1/2 w_2$ is a locator set for A. Suppose that $A = S - S$, where S is convex. Then some translate of S, call it S', is contained in L'. Since $w_1 \in A$ there exist $u, v \in S'$ such that $w_1 = u - v$. Since $S' \subseteq L'$, then $u, v \in L'$. It follows that $u = 1/2 w_1$ and $v = -1/2 w_1$. Therefore $1/2 w_1 \in S'$ and $-1/2 w_1 \in S'$. Similarly, $1/2 w_2 \in S'$ and $-1/2 w_2 \in S'$. Then, since S' is convex,

$$L' = \text{c.hull}\,[\{1/2 w_1, -1/2 w_1, 1/2 w_2, -1/2 w_2\}] \subseteq S' \subseteq L'. \tag{26}$$

Therefore $S' = L' = 1/2 A$, and so S is unique among convex solutions.

It can also be shown that parallelograms are the *only* two-dimensional convex-unambiguous sets, and convex-symmetric sets $A = \subseteq E^2$ that are not parallelograms can be shown to have infinitely many nonequivalent solutions to $A = S - S$. The lengthy proof of this last result is omitted here for the sake of brevity.

5. AUTOCORRELATION TRI-INTERSECTION FOR COLLECTIONS OF POINTS

For the special case of certain finite sets consisting of a collection of distinct points, the solution can be generated by a method similar to the one for convex sets. For example, the function

$$f(x) = \sum_{m=1}^{M} f_m \delta(x - x_m) \tag{27}$$

consisting of M delta functions having amplitudes $f_m > 0$, at the distinct points $x_m \in E^N$, $m = 1, \ldots, M$, would have support

$$S = \{x_m : m = 1, \ldots, M\}. \tag{28}$$

Let S be a set consisting of a collection of distinct points and let $A = S - S$. Define the following three conditions on the set S, which are needed for the results that follow.

Condition 1:
Whenever

$$x_1, x_2, y_1, y_2, z_1, z_2, \in S, \qquad x_1 \neq x_2,$$
$$x_1 - x_2 + y_1 - y_2 + z_1 - z_2 = 0, \tag{29}$$

then $x_1 = y_2$ or $x_1 = z_2$, and $x_2 = y_1$ or $x_2 = z_1$.

Condition 2:
Whenever the set $G \subseteq A$ consists of three distinct points, and $0 \in G$ and $G - G \subseteq A$, then G is equivalent to a subset of S.

Condition 3:
Whenever $x_1, x_2, y_1, y_2 \in S$, $x_1 \neq x_2$, and $x_1 - x_2 = y_1 - y_2$, then $x_1 = y_1$.

The meaning of Conditions 1 and 3 is discussed in Section 7. Condition 3 is equivalent to saying that no two vector spacings between any distinct pairs of points in S are equal.

Now define the set B as follows: Let $w_1 \in A$ and $w_2 \in A \cap (w_1 + A)$, with $0 \neq w_1 \neq w_2 \neq 0$, and let

$$B = A \cap (w_1 + A) \cap (w_2 + A). \tag{30}$$

We have the following three results, which hold for any number of dimensions:

(1) If S satisfies Condition 1, then

$$S \sim B. \tag{31}$$

That is, B is the unique solution to $A = S - S$.

(2) If S satisfies Condition 2, then S is equivalent to a subset of B.

(3) If S satisfies Conditions 2 and 3, then again $S \sim B$. In fact, S satisfies Conditions 2 and 3 if and only if it satisfies Condition 1.

The proofs of these three results are given in Appendix C. Since it requires a special relationship between the points in S in order to violate Condition 1, it is probable that for S composed of randomly located points, B is the unique solution to $A = S - S$. More will be said about this later.

Example 5

Consider the set S consisting of the collection of nine points shown in Fig. 7(a). $A = S - S$ shown in Fig. 7(b) has $9^2 - 9 + 1 = 73$ points. Intersecting A with a translate of itself by using Eq. (12), a number of different locator sets L for A can be formed, two of which are shown in Figs. 7(c) and 7(d). (Each locator set must contain some translate of any solution

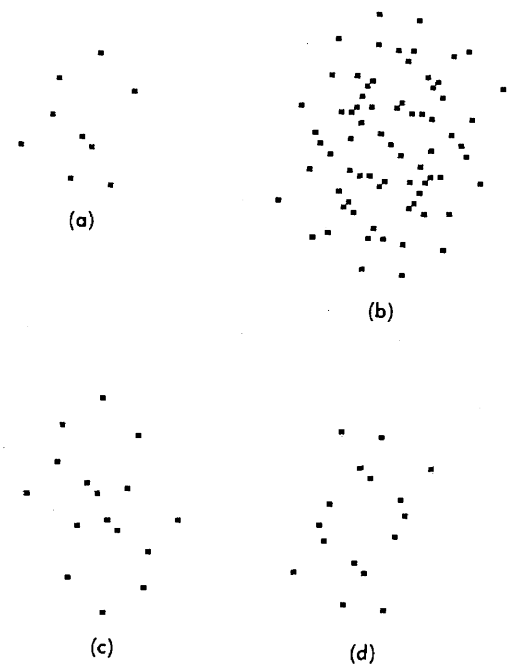

Fig. 7. Autocorrelation tri-intersection for sets consisting of a collection of distinct points. (a) Set S, (b) $A = S - S$, (c) and (d) locators of the form $L = A \cap (w + A)$. Intersecting (c) or (d) with (b) yields the unique solution (a).

to $A = S - S$.) Taking the intersection of L in either Fig. 7(c) or Fig. 7(d) with a translate of A centered on any point within L yields, according to Eq. (30), the solution B, which is found to be equivalent to S in Fig. 7(a). For this example, for all allowable values of w_1 and w_2, B is found to be equivalent to S, which is shown in Fig. 7(a); that is, the solution B is unique.

Example 6

Consider the set S consisting of the collection of nine points shown in Fig. 8(a). The positions of eight of the points in S are identical to those of eight of the points of the set shown in Fig. 7(a). The ninth point in S (in the lower center) was moved in such a way as to make the vector spacing equal between two pairs of four distinct points. That is, there are four distinct points x_1, x_2, y_1, and y_2 in S satisyfing $x_1 - x_2 = y_1 - y_2$. This violates Condition 3 and hence also Condition 1. Therefore $B - B$ is not necessarily equal to A, where B is given by Eq. (30). $A = S - S$ shown in Fig. 8(b) has only 69 points, compared with 73 for the previous example. The redundancy of the vector spacings (the differences) in S results in a twofold redundancy in four of the points of A (at $x_1 - x_2 = y_1 - y_2$, $x_2 - x_1 = y_2 - y_1$, $x_1 - y_1 = x_2 - y_2$, and $y_1 - x_1 = y_2 - x_2$). Figures 8(c)–8(e) show three of the locator sets for A that are formed by using Eq. (12). Once again, each locator set must contain some translate of any solution of $A = S - S$. Therefore for any solution there must exist a point v such that a translate of the solution is a subset of $L_1 \cap (v + L_2)$, where L_1 and L_2 are locator sets for A. In addition, S must contain at least nine points, since if it contained only eight points, then A could contain at most $8^2 - 8 + 1 = 57$ points. Trying all possible translations of the locator set shown in Fig. 8(d), only two of its intersections with the locator set shown in Fig. 8(c) have at least nine points: set S_1, shown in Fig. 8(f), and a translate of $-S_1$. Any solution therefore must be equivalent to S_1 or to a subset of S_1. $S_1 - S_1$ is found to have more than

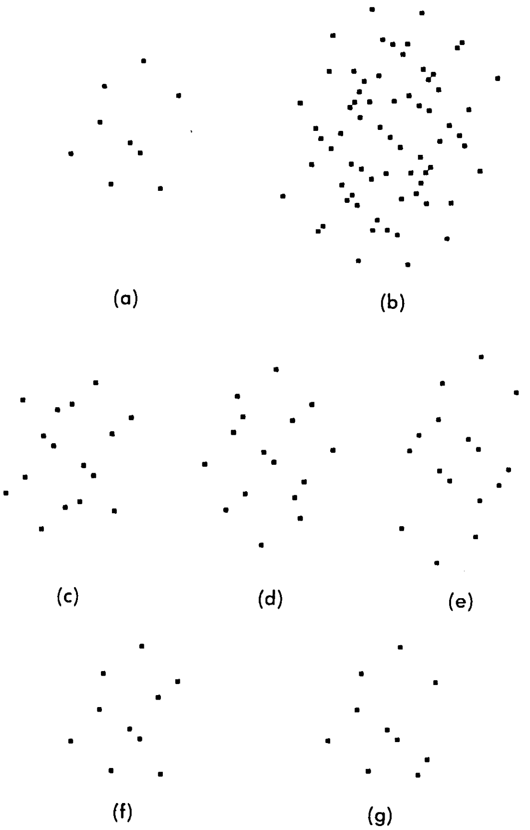

Fig. 8. Autocorrelation intersection for redundant case. (a) Set S, (b) $A = S - S$, (c)–(e) locators of the form $L = A \cap (w + A)$, (f) intersection of (c) with (d), (g) another intersection of three translates of A.

the 69 points in A, and $A \subset S_1 - S_1$. Therefore, since S_1 has ten points and any solution must have at least nine points, it follows that any solution must have exactly nine points. Trying other pairs of locator sets for A, depending on the pair of locator sets chosen, we often get intersections containing ten points, but the tenth point will be different, such as in the set shown in Fig. 8(g). The only possible solution is obviously S in Fig. 8(a) (that is, the solution is unique), since it is the only nine-point set that is equivalent to subsets of both the sets shown in Figs. 8(f) and 8(g). Furthermore, if one takes intersections of translates of the two particular locator sets shown in Figs. 8(c) and 8(e), then the only resulting set of nine or more points is S in Fig. 8(a); that is, by the lucky choice of which two locator sets to intersect, the solution can be found immediately. Equivalently, it can be shown that there are values of w_1 and w_2 such that $B \sim S$, although that is not true for most values of w_1 and w_2.

Therefore, even when Condition 1 is not satisfied, it is sometimes possible to find solutions (and the solution may even be unique, as it was in Example 6) by intersecting three or more translates of A. However, when Condition 1 is not satisfied, then there is no guarantee that the solution is unique, and finding solutions is considerably more complicated than simply evaluating B by Eq. (30). Unfortunately, given A it is not possible to determine immediately whether Condition 1 is satisfied. A necessary condition that Condition 1 (or Condition 3) be satisfied is that the number of points in A can be expressed as $M^2 - M + 1$, where $M \geq 1$ is an integer.

6. RECONSTRUCTION OF OBJECTS CONSISTING OF COLLECTIONS OF POINTS

By a simple modification of the method described in the previous section for reconstructing the support of an object consisting of a collection of distinct points, it is often possible to reconstruct the object itself. The method is analogous to using Eq. (30) to compute B. Recall that in computing B one takes the intersection of three translates of the autocorrelation support. If one takes the product of three translates of the autocorrelation function of $f(x)$, using the same translations as are used to compute B, then the support of that product will be B. And if, as described earlier, Condition 1 is satisfied, then B is a solution to $A = S - S$, and therefore the support of that product is equivalent to the support of $f(x)$. In what follows it is shown that when Condition 1 is satisfied, $f(x)$ can be reconstructed from that product in a simple way [by using Eqs. (38)–(40)].

Suppose that the object is given by Eq. (27), consisting of M delta functions located at the distinct points x_m having amplitudes f_m, $m = 1, 2, \ldots, M$. The positions x_m are vectors in any number of dimensions. The autocorrelation is

$$f \star f(x) = \int_{E^N} f(y) f(y + x) \mathrm{d}y = \sum_{n=1}^{M} \sum_{m=1}^{M} f_n f_m \delta(x - x_m + x_n), \tag{32a}$$

which can be expressed as

$$f \star f(x) = \sum_{n=1}^{M} f_n^2 \delta(x) + \sum_{n=1}^{M} \sum_{m \neq n}^{M} f_n f_m \delta(x - x_m + x_n), \tag{32b}$$

which has M^2 terms located at positions $x = x_m - x_n$, M of which are at $x = 0$. That is, it has up to $M^2 - M + 1$ distinct terms. For this type of object, the fact that the support of the autocorrelation is given by $A = S - S$ is obvious from Eqs. (32).

Here we would like to take the product of two such autocorrelation functions; however, the product of the two delta functions is not well defined. Several approaches to overcome this difficulty are possible. For simplicity we define the product of two delta functions as follows:

$$[a\delta(x - x_1)][b\delta(x - x_2)] = \begin{cases} ab\delta(x - x_1), & x_2 = x_1 \\ 0, & x_2 \neq x_1 \end{cases} \tag{33}$$

It is intuitively helpful to think of $f(x)$ in Eq. (27) as a digitized array of sampled values, with the values f_m at addresses x_m, $m = 1, 2, \ldots, M$. Then the delta functions in this section can be thought of as Kronecker delta functions.

As a first step toward forming a product analogous to B of Eq. (30), we consider the product of $f \star f(x)$ and $f \star f(x - w)$, where $w \in A$, and we choose $w \neq 0$. From Eq. (32) it is evident that $w \in A$ is of the form $x_j - x_k$, where $x_j, x_k \in S$. Therefore, we are taking the product of $f \star f(x)$ and $f \star f(x - x_j + x_k)$, where $x_j - x_k \neq 0$ lies within the support of $f \star f(x)$. The center of the translated autocorrelation lies within the support of the untranslated autocorrelation. By using Eq. (32b), the autocorrelation product is (all summations are from

1 to M unless otherwise noted)

$$\begin{aligned}AP_{jk}(x) &= [f \star f(x)][f \star f(x - x_j + x_k)]\\
&= \left[\left(\sum_n f_n{}^2\right)\delta(x) + \sum_n \sum_{m\neq n} f_n f_m \delta(x - x_m + x_n)\right]\\
&\quad \times \left[\left(\sum_n f_n{}^2\right)\delta(x - x_j + x_k)\right.\\
&\quad + \sum_{n'}\sum_{m'\neq n'} f_{n'} f_{m'}\\
&\quad \left.\times\, \delta(x - x_{m'} + x_{n'} - x_j + x_k)\right] \qquad (34a)\\
&= \left(\sum_n f_n{}^2\right) f_j f_k \delta(x) + \left(\sum_n f_n{}^2\right) f_j f_k \delta(x - x_j + x_k)\\
&\quad + f_j f_k \sum_{m\neq k,j} f_m{}^2 \delta(x - x_m + x_k)\\
&\quad + f_j f_k \sum_{n\neq k,j} f_n{}^2 \delta(x - x_j + x_n) + (\mathrm{OT}), \qquad (34b)\end{aligned}$$

where (OT) denotes other terms, as will be described later. [As an example of how Eq. (34b) follows from Eq. (34a), the fourth term in Eq. (34b) arises from the product of the second term of the first autocorrelation with the second term of the second autocorrelation, with $m = j$, $n' = n$ and $m' = k$.] By using Eq. (32a), another way of expressing Eq. (34) is

$$\begin{aligned}AP_{jk}(x) = \sum_n \sum_m \sum_{n'} \sum_{m'} f_n f_m f_{n'} f_{m'} \delta(x - x_m + x_n)\\
\times\, \delta(x - x_{m'} + x_{n'} - x_j + x_k), \quad (34c)\end{aligned}$$

from which it is seen that terms survive at points x where

$$x = x_m - x_n = x_{m'} - x_{n'} + x_j - x_k. \qquad (35)$$

The terms shown in Eq. (34b) all necessarily appear. In addition, other terms may appear, as indicated by the expression +(OT). The existence of other terms depends on the presence of special relationships between the coordinates x_n, thus allowing Eq. (35) to be satisfied by chance. There being no additional terms is equivalent to Condition 1 (described in Section 5) being satisfied. If the x_m were independent random variables, then the chance of having additional surviving terms would be small, and we would have (OT) = 0.

Combining Eq. (27) with Eq. (34b), the autocorrelation product can be expressed as

$$\begin{aligned}AP_{jk}(x) &= f_j f_k\, [f^2(x + x_k) + f^2(-x + x_j)]\\
&\quad + \left(\sum_{n\neq k,j} f_n{}^2\right) f_j f_k [\delta(x) + \delta(x - x_j + x_k)] + (\mathrm{OT}). \quad (36)\end{aligned}$$

Therefore there are translates of the supports of both $f(x)$ and $f(-x)$ that are contained within the support of $AP_{jk}(x)$. This can also be seen from the fact that by Eq. (12) the support of $AP_{jk}(x)$ is a locator set.

Now consider the second step toward forming a product analogous to B of Eq. (30): we take the product of $AP_{jk}(x)$ with a third autocorrelation $f \star f(x - w')$, where w' is within the support of $AP_{jk}(x)$. Suppose that (OT) = 0. Then from Eq. (34b) it is seen that the support of $AP_{jk}(x)$ consists of the points $x_n - x_k$ and $x_j - x_n$, $n = 1, 2 \ldots, M$. We first take the case in which w' is of the form $x_n - x_k$ and treat the case of $w' = x_j - x_n$ later. Suppose that the specific point chosen is for $n = j' \neq j, k$ (i.e., $w' = x_{j'} - x_k \neq 0$, and $w' \neq w = x_j - x_k$). Then the product of the three autocorrelations is

$$\begin{aligned}AP_{jkj'k}(x) &= [f \star f(x)][f \star f(x - x_j + x_k)]\\
&\quad \times [f \star f(x - x_{j'} + x_k)]\\
&= AP_{jk}(x)[f \star f(x - x_{j'} + x_k)]\\
&= f_j f_k \left[\left(\sum_n f_n{}^2\right)\delta(x) + \left(\sum_n f_n{}^2\right)\delta(x - x_j + x_k)\right.\\
&\quad + \sum_{n\neq k,j} f_n{}^2 \delta(x - x_n + x_k)\\
&\quad \left.+ \sum_{n\neq k,j} f_n{}^2\, \delta(x - x_j + x_n)\right]\\
&\quad \times \left[\left(\sum_n f_n{}^2\right)\delta(x - x_{j'} + x_k)\right.\\
&\quad \left.+ \sum_{n'}\sum_{m'\neq n'} f_{n'} f_{m'} \delta(x - x_{m'} + x_{n'} - x_{j'} + x_k)\right]\\
&= f_k f_j f_{j'} \left\{\sum_{n\neq k,j,j'} f_n{}^3 \delta(x - x_n + x_k)\right.\\
&\quad + \left(\sum_n f_n{}^2\right)[f_k \delta(x) + f_j \delta(x - x_j + x_k)\\
&\quad \left.+ f_{j'} \delta(x - x_{j'} + x_k)]\right\} \qquad (37a)\\
&= f_k f_j f_{j'} \left[f^3(x + x_k) + \left(\sum_{n\neq k} f_n{}^2\right) f_k \delta(x)\right.\\
&\quad + \left(\sum_{n\neq j} f_n{}^2\right) f_j \delta(x - x_j + x_k)\\
&\quad \left.+ \left(\sum_{n\neq j'} f_n{}^2\right) f_j \delta(x - x_{j'} + x_k)\right]. \qquad (37b)\end{aligned}$$

That is, the product of three autocorrelations has the same support as $f(x + x_k)$, as was shown earlier in connection with Eq. (30), since B is just the support of the product of three such autocorrelation functions. Furthermore, except at the three points $x = 0$, $x_j - x_k$, and $x_{j'} - x_k$, the product is proportional to the cube of $f(x + x_k)$.

The values at all points can be determined as follows: First,

$$D \equiv \sum_n f_n{}^2 = f \star f(0) \qquad (38)$$

is known, so that factor can be divided out from the last three terms of Eq. (37a). Second, let the coefficients of those three terms in Eq. (37a) be (with Σf_n^2 divided out)

$$A = D^{-1} AP_{jkj'k}(0) = f_k{}^2 f_j f_{j'}, \qquad (39a)$$

$$B = D^{-1} AP_{jkj'k}(x_j - x_k) = f_k f_j{}^2 f_{j'}, \qquad (39b)$$

$$C = D^{-1} AP_{jkj'k}(x_{j'} - x_k) = f_k f_j f_{j'}{}^2. \qquad (39c)$$

Solving, we get

$$f_k = \left(\frac{A^3}{BC}\right)^{1/4}, \qquad (40a)$$

$$f_j = \left(\frac{B^3}{AC}\right)^{1/4}, \qquad (40b)$$

$$f_{j'} = \left(\frac{C^3}{AB}\right)^{1/4}, \tag{40c}$$

and

$$f_k f_j f_{j'} = (ABC)^{1/4}. \tag{40d}$$

The remaining values of f_m, for $m \neq k, j, j'$, can then be computed by dividing Eq. (37a) by $f_k f_j f_{j'}$ and then taking the cube root:

$$f_m = \left[\frac{AP_{jkj'k}(x_m - x_k)}{f_k f_j f_{j'}}\right]^{1/3}. \tag{40e}$$

By this method $f(x)$ is reconstructed exactly to within a translation, as long as (OT) = 0.

In performing these calculations, had we chosen a second translation of the form $(x_j - x_{k'})$, $k' \neq k, j$ instead of $(x_{j'} - x_k)$, then the result would have been similar, except a translate of $f(-x)$ instead of a translate of $f(x)$ would have been reconstructed. If (OT) $\neq 0$, that is, if Condition 1 is not satisfied, then additional terms appear that make the analysis much more complicated and may prevent the reconstruction of $f(x)$.

Various modifications to this reconstruction method are possible. For example, the product of two autocorrelation products $AP_{jk}(x)\, AP_{j'k}(x)$ is proportional to $f^4(x + x_k)$ except at three points. Another example is to define the autocorrelation support function as

$$A(x) = \delta(x) + \sum_{n=1}^{M} \sum_{m \neq n} \delta(x - x_m + x), \tag{41}$$

which is just a binary-valued version of Eq. (32b). Then the product of the autocorrelation function with two properly translated autocorrelation support functions is proportional to a translate of $f(x)$, except at a single point that can be determined by an extra few simple steps.

7. OTHER TERMS

In arriving at Eq. (37), it was assumed that the other terms (OT) = 0, or equivalently that Condition 1 be satisfied. The terms included in Eqs. (34b) and (37) are those that necessarily arise by satisfying

$$x_m - x_n = x_{m'} - x_{n'} + x_j - x_k \tag{42}$$

trivially, for example, for $m = n$, $m' = k$, and $n' = j$. The other terms are those that satisfy Eq. (42) by chance, that is, those that arise in addition to those that (trivially) arise necessarily. The trivial solutions are the ones mentioned in connection with Condition 1 in Section 5. These other terms require a special relationship between the points in S and would not be expected to occur if the points in S are randomly distributed in some region of E^N.

Figure 9 shows in two dimensions some relationships between points in S that would cause Eq. (42) to be satisfied by chance, that is to say, in a nontrivial way. (S may contain additional points that are not shown.) For example, if the chords between three pairs of six distinct points in S as shown in Fig. 9(a) can be translated to form a triangle as shown in Fig. 9(b), then Eq. (42) is satisfied nontrivially. A similar result holds if some of the endpoints of the three chords are the same points, except for the trivial case of three points already in the form of a triangle defining the three chords. Note that when

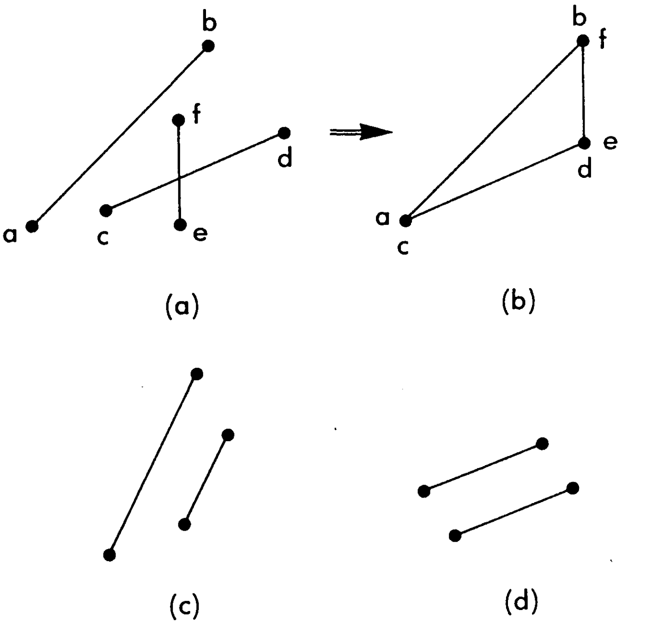

Fig. 9. Redundancy types of relationships within S that would violate Condition 1. (a) and (b) three vector separations add to zero, (c) one vector separation is twice another, (d) two vector separations are equal.

$m' = j$ and $n' = k$, then Eq. (42) reduces to $x_m - x_n = 2(x_j - x_k)$. That is, another nontrivial case is the existence of a vector separation between one pair of points equaling twice the vector separation between another pair of points, as shown in Fig. 9(c). Also note that when, say, $m' = n'$, then Eq. (42) reduces to $x_m - x_n = x_j - x_k$. That is, another nontrivial case is the existence of a vector separation between one pair of points equaling the vector separation between a different pair of points, as shown in Fig. 9(d). This last case is also a violation of Condition 3 (see the discussion in Section 5) and an example of that case was shown in Example 6 and depicted in Fig. 8.

As was mentioned earlier, if the points x_m, $m = 1, 2, \ldots, M$ are randomly distributed, then it would be unlikely that any of these special relationships exist, and so one would expect that (OT) would equal zero and Condition 1 would be satisfied.

These results, with some modifications, can also be extended to the case of an object having support on a number of disjoint islands having diameters small compared with their separations (as opposed to the support consisting of isolated mathematical points). However, as the number of islands increases and as the ratio of the diameters of the islands to their separations increases, the probability of satisfying a condition analogous to Condition 1 decreases.

8. SUMMARY

We have described a number of new results relating to the reconstruction of the support of an object function from the support of its autocorrelation. Locator sets that contain all possible solutions were described, the most interesting of which is the intersection of the autocorrelation support with a translate of itself. For the special case of convex sets in two dimensions, it was shown that the intersection of three translates of the autocorrelation support is a solution. These solutions can usually be combined to form still more solutions. Among convex sets in two dimensions, only parallelograms have unique solutions. For the case of objects consisting of collections of distinct points, it was shown that unless a special relationship exists between the points in the object, the intersection of three translates of the autocorrelation support yields the solution, and it is unique. If, instead of intersecting autocorrelation supports, one takes the product of translated autocorrelation functions, then for the same objects consisting of collections of points one can easily reconstruct the object function itself.

Some of the results on objects consisting of collections of distinct points are also described in Ref. 5. These results were first presented[6] at the Annual Meeting of the Optical Society of America in Chicago, Illinois, in October 1980.

APPENDIX A.

If the support of $f(x)$ is S, then the support of $f(y+x)$ is $S-y$. Then the interpretation of Eq. (1) as the weighted sum of $f(y+x)$ with weights $f(y)$ leads intuitively to the fact that A, the support of $f\bigstar f(x)$, is given by

$$A = \bigcup_{y\in S} (S-y) = S-S.$$

A rigorous proof for compact sets S is as follows: Define

$$B(x,r) = \{y \in E^N : |x-y| \le r\}$$

and

$$f_r(x) = \int_{B(x,r)} f(y)dy.$$

Then $x \in S$ if and only if $f_r(x) > 0$ for all $r > 0$. Also, if $|x-y| < r$, then $f_{2r}(y) \ge f_r(x)$.

Part 1: $S - S \subseteq A$

Let $x, y \in S$ and let $r > 0$. Then

$$\begin{aligned}(f\bigstar f)_{2r}(x-y) &= \int_{B(x-y,2r)} f\bigstar f(p)\mathrm{d}p \\ &= \int_{B(0,2r)}\int_{E^N} f(w) \\ &\quad \times f(w+p+x-y)\mathrm{d}w\mathrm{d}p \\ &= \int_{E^N} f(w)\, f_{2r}(w+x-y)\mathrm{d}w \\ &= \int_{E^N} f(w+y) f_{2r}(w+x)\mathrm{d}w \\ &\ge \int_{B(0,r)} f(w+y) f_{2r}(w+x)\mathrm{d}w \\ &\ge f_r(x)\int_{B(0,r)} f(w+y)\mathrm{d}w \\ &= f_r(x) f_r(y) > 0.\end{aligned}$$

Therefore, since $r > 0$ was arbitrary, $x - y \in A$, and so $S - S \subseteq A$.

Part 2: $A \subseteq S - S$

First, note that since S is compact, $S - S$ is a closed set. Let $x \in A$ and let $r > 0$. Then

$$\begin{aligned}0 < (f\bigstar f)_r(x) &= (f\bigstar f)_r(-x) \\ &= \int_{B(-x,r)} f\bigstar f(p)\mathrm{d}p \\ &= \int_{B(0,r)}\int_{E^N} f(y)f(y+p-x)\mathrm{d}y\mathrm{d}p \\ &= \int_{B(0,r)}\int_{E^N} f(y+p)f(y+x)\mathrm{d}y\mathrm{d}p \\ &= \int_{E^N} f_r(y)f(y+x)\mathrm{d}y.\end{aligned}$$

Therefore there exists $z \in E^N$ such that

$$\begin{aligned}0 &< \int_{B(z,r)} f_r(y)f(y+x)\mathrm{d}y \\ &< f_{2r}(z)\int_{B(z,r)} f(y+x)\mathrm{d}y \\ &= f_{2r}(z) f_r(z+x).\end{aligned}$$

Therefore $f_{2r}(z) > 0$ and $f_r(z+x) > 0$. Hence $S \cap B(z, 2r) \ne \phi$ and $S \cap B(y,r) \ne \phi$, where $y = z + x$. Choose $z' \in S \cap B(z, 2r)$ and $y' \in S \cap B(y,r)$. Then $|y'-y| < r$ and $|z'-z| < 2r$. Then $|(y'-z')-x| = |(y'-y)-(z'-z)| \le |y'-y| + |z'-z| < 3r$. Since $r \ge 0$ was arbitrary, $S - S$ is closed, and $y' - z' \in S - S$, it follows that $x \in S - S$, and hence $A \subseteq S - S$, and hence $A = S - S$.

APPENDIX B. PROOF THAT $A = B - B$ FOR CONVEX SETS

The proof that $A = B - B$ will be divided into two parts. First, it will be shown that $A \subseteq B - B$, and then it will be shown that $A \supseteq B - B$.

Part 1: $A \subseteq B - B$

It can be shown that, because A has nonnull interior, the points 0, w_1, and w_2 are not collinear. Let

$$B_1 = \text{c.hull}\,\{0, w_1, w_2\}.$$

Since B is the intersection of three convex sets, B is convex. Therefore $B_1 \subseteq B$. Let $A_1 = B_1 - B_1$.

Claim 1: $A_1 \subseteq A$

As can be seen from Fig. 10, we have

$$A_1 = \text{c.hull}\,(w_1, -w_1, w_2, -w_2, w_1 - w_2, w_2 - w_1).$$

Furthermore, since A is convex and

$$w_1, -w_1, w_2, -w_2, w_1 - w_2, w_2 - w_1 \in A,$$

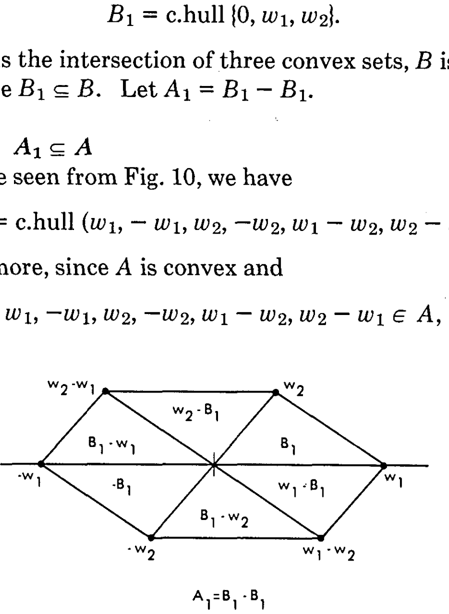

Fig. 10. $A_1 = \text{c. hull}\{w_1, -w_1, w_2, -w_2, w_1 - w_2, w_2 - w_1\}$, and $A_1 \subseteq A$. This and Figs. 11–19 illustrate steps in the proof that $A = B - B$.

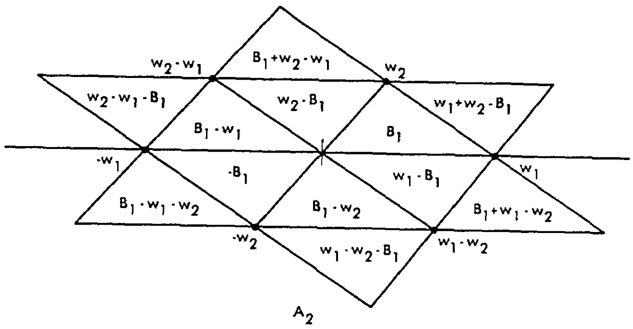

Fig. 11. The set A_2.

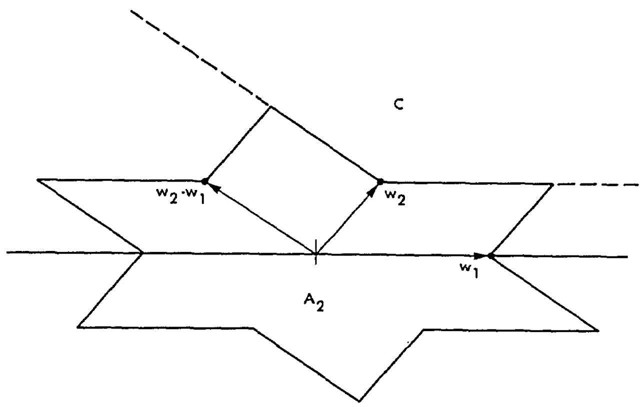

Fig. 12. C is one of the extended "notches" in A_2.

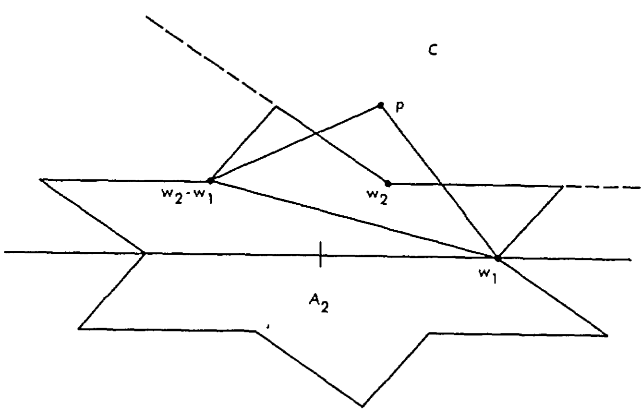

Fig. 13. Illustration of $w_2 \in \text{int}(D)$, where $D = \text{c. hull}\,\{p, w_1, w_2 - w_1\}$ is used to prove that $A \cap C = 0$ and therefore $A \subseteq A_2$.

it follows that $A_1 \subseteq A$. This completes the proof of Claim 1.

Now let

$$A_2 = A_1 \cup (B_1 - w_1 - w_2) \cup (B_1 + w_2 - w_1) \cup (B_1 + w_1 - w_2) \cup (w_1 + w_2 - B_1) \cup (w_1 - w_2 - B_1) \cup (w_2 - w_1 - B_1).$$

See Fig. 11.

Claim 2: $A \subseteq A_2$.
Let

$$C = \{w_2 + \lambda_1 w_1 + \lambda_2(w_2 - w_1):\ \lambda_1 > 0 \text{ and } \lambda_2 > 0\}.$$

See Fig. 12. Note that C is an open set. We will show that $A \cap C = \phi$. Suppose that $A \cap C \neq \phi$. Then let $p \in A \cap C$ and let $D = \text{c.hull}\,\{p, w_1, w_2 - w_1\}$. See Fig. 13. Then $D \subseteq A$ and $w_2 \in \text{int}(D) \subseteq \text{int}(A)$. This contradicts the assumption that $w_2 \in \partial(A)$. Therefore $A \cap C = \phi$.

Similar arguments apply to the other notches in A_2. Therefore $A \subseteq A_2$. This completes the proof of Claim 2.

Summarizing, we have $B_1 \subseteq B$ and $A_1 \subseteq A \subseteq A_2$.

Let $p \in A$. We want to show that $p \in B - B$. We have

$$\begin{aligned} A \subseteq A_2 = {} & [B_1 \cup (w_1 + w_2 - B_1)] \\ & \cup [(-B_1) \cup (B_1 - w_1 - w_2)] \\ & \cup [(B_1 - w_1) \cup (w_2 - w_1 - B_1)] \\ & \cup [(w_1 - B_1) \cup (B_1 + w_1 - w_2)] \\ & \cup [(B_1 - w_2) \cup (w_1 - w_2 - B_1)] \\ & \cup [(w_2 - B_1) \cup (B_1 + w_2 - w_1)]. \end{aligned}$$

Case 1: $p \in B_1 \cup (w_1 + w_2 - B_1)$
We have

$$p - w_1 \in (B_1 - w_1) \cup (w_2 - B_1) \subseteq A_1 \subseteq A.$$

Therefore $p \in w_1 + A$. Also, $p - w_2 \in (B_1 - w_2) \cup (w_1 - B_1) \subseteq A_1 \subseteq A$. Therefore $p \in w_2 + A$. Since, by assumption, $p \in A$, it follows that $p \in B$. We also have $0 \in B$. Therefore $p = p - 0 \in B - B$.

Case 2: $p \in (-B_1) \cup (B_1 - w_1 - w_2)$
We have $-p \in B_1 \cup (w_1 + w_2 - B_1)$. Therefore, by Case 1, $-p \in B - B$, and since $B - B$ is a symmetric set, $p \in B - B$.

In the four other cases, i.e., $p \in (B_1 - w_1) \cup (w_2 - w_1 - B_1)$, etc., we find that $p \in B - B$ by similar arguments. This completes the proof of Part 1.

Part 2: $A \supseteq B - B$
Let l_1, l_2, l_3 be lines tangent to A at points w_1, w_2, and $w_1 - w_2$, respectively. See Fig. 14. Then, since A is symmetric, the lines $-l_1$, $-l_2$, and $-l_3$ are tangent to A at points $-w_1$, $-w_2$, and $w_2 - w_1$, respectively.

It follows that $w_1 - l_1$ is tangent to $w_1 + A$ at 0. Therefore $w_1 - l_1$ is tangent to B at 0. See Fig. 15. Similarly, $w_2 - l_2$ is tangent to $w_2 + A$ at 0. Hence $w_2 - l_2$ is tangent to B at 0. Also, $w_2 + l_3$ is tangent to $w_2 + A$ at w_1. Therefore, $w_2 + l_3$ is tangent to B at w_1. Finally, $w_1 - l_3$ is tangent to $w_1 + A$ at

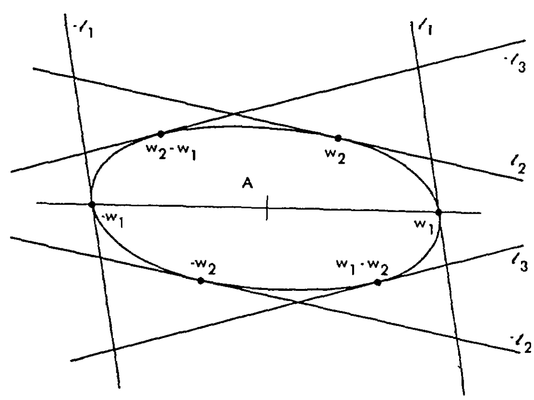

Fig. 14. The lines $l_1, -l_1, l_2, -l_2, l_3$, and $-l_3$ are tangent to the set A at points $w_1, -w_1, w_2, -w_2, w_1 - w_2$, and $w_2 - w_1$, respectively.

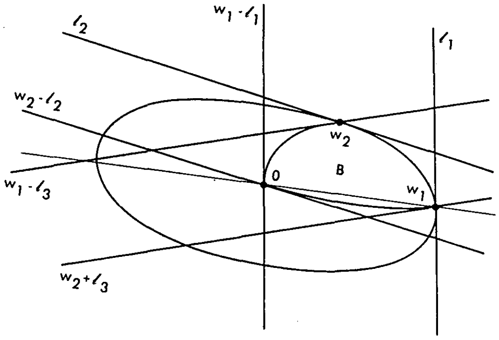

Fig. 15. The set B lies between lines l_1 and $w_1 - l_1$, between l_2 and $w_2 - l_2$, and between $w_2 + l_3$ and $w_1 - l_3$.

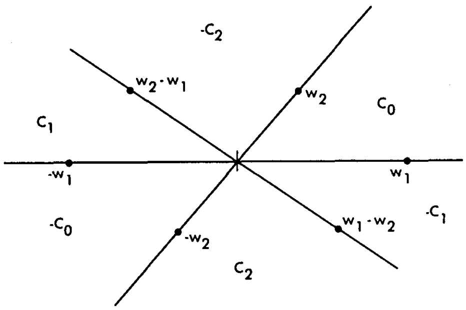

Fig 16. The entire plane is the union of the cones C_0, $-C_0$, C_1, $-C_1$, C_2, and $-C_2$.

w_2. Therefore, $w_1 - l_3$ is tangent to B at w_2. It follows that B lies between lines l_1 and $w_1 - l_1$ and between l_2 and $w_2 - l_2$ and between $w_2 + l_3$ and $w_1 - l_3$.

Now let C_0 be the closed positive cone spanned by w_1 and w_2. That is,

$$C_0 = \{\lambda_1 w_1 + \lambda_2 w_2\colon\ \lambda_1 \geq 0 \text{ and } \lambda_2 \geq 0\}.$$

See Fig. 16. Let C_1 be the closed cone spanned by $-w_1$ and $w_2 - w_1$. Finally, let C_2 be the closed positive cone spanned by $-w_2$ and $w_1 - w_2$. Then

$$E^2 = C_0 \cup (-C_0) \cup C_1 \cup (-C_1) \cup C_2 \cup (-C_2).$$

Next, let

$$s_0 = C_0 \cap \partial(B),$$
$$s_1 = (w_1 + C_1) \cap \partial(B),$$
$$s_2 = (w_2 + C_2) \cap \partial(B).$$

Then $\partial(B) = s_0 \cup s_1 \cup s_2$. See Fig. 17.

Now let $p_1, p_2 \in B$. We want to show that $p_1 - p_2 \in A$.

Case 1: $p_1 - p_2 \in C_2$

First, if $p_1 = p_2$, then $p_1 - p_2 = 0 \in A$.

Now assume that $p_1 \neq p_2$. Let l be the (infinite) line passing through p_1 and p_2. See Fig. 18. The line l must intersect either s_0 or s_1.

Subcase 1a: l Intersects s_0

See Fig. 18. Let l'_2 be the line parallel to l_2 and passing through p_1. Let l''_2 be the line parallel to l_2 and passing through p_2.

Now lines l'_2 and l''_2 lie between l_2 and $w_2 - l_2$. Also, 0 is on $w_2 - l_2$ and w_2 is on l_2. It follows that l'_2 and l''_2 must intersect the line segment $[0, w_2]$. Let r_1 be the point at which l'_2 intersects $[0, w_2]$, and let r_2 be the point at which l''_2 intersects $[0, w_2]$. Then, since $0, w_2 \in B$ and B is convex, $r_1 \in B$ and $r_2 \in B$.

Now let l' be the line parallel to l and passing through w_2. Since $p_1 - p_2 \in C_2$, l cannot be parallel to l_2. Therefore l' is not parallel to l'_2 or to l''_2. It follows that l' intersects l'_2 and l''_2. Let q_1 be the point of intersection of l' and l'_2 and let q_2 be the point of the intersection of l' and l''_2.

Since l intersects s_0, it follows that $q_1 \in [p_1, r_1]$ and $q_2 \in [p_2, r_2]$. Since $p_1, p_2, r_1, r_2 \in B$ and B is convex, it follows that $q_1 \in B$ and $q_2 \in B$.

Now, since $p_1 - p_2 \in C_2$, we must have $q_2 \in [q_1, w_2]$. That is, there exists λ, $0 \leq \lambda \leq 1$, such that $q_2 = \lambda q_1 + (1 - \lambda) w_2$ or $q_2 - w_2 = \lambda(q_1 - w_2)$.

Now $q_1 \in B \subseteq w_2 + A$. Therefore $q_1 - w_2 \in A$. Furthermore, since $0 \leq 1 - \lambda \leq 1$, it follows that $(1 - \lambda)(q_1 - w_2) \in A$. Finally, we have

$$\begin{aligned} p_1 - p_2 &= q_1 - q_2 \\ &= (q_1 - w_2) - (q_2 - w_2) \\ &= (1 - \lambda)(q_1 - w_2) \in A. \end{aligned}$$

This completes the proof of Subcase 1a.

Subcase 1b: l Intersects s_1

See Fig. 19. An argument similar to the above is indicated in Fig. 19. This completes the proof of Case 1.

Case 2: $p_2 - p_2 \in -C_2$

We have $p_2 - p_1 \in C_2$. Therefore, by Case 1, $p_2 - p_1 \in A$, and hence $p_1 - p_2 \in A$.

Similar arguments apply when $p_1 - p_2 \in C_0, -C_0, C_1$, and $-C_1$. This completes Part 2 of the proof that $A = B - B$ for convex sets.

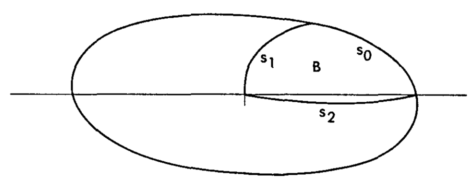

Fig. 17. The boundary of B is the union of the arcs s_0, s_1, and s_2.

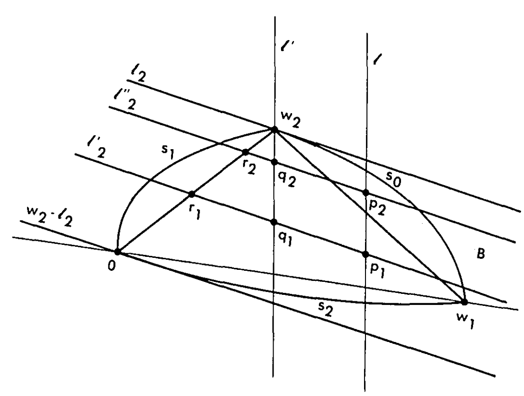

Fig. 18. Illustration of the proof that $p_1 - p_2 \in A$ when the line l intersects the arc s_0 and $p_1 - p_2$ is in the cone C_2 (illustrated in Fig. 16).

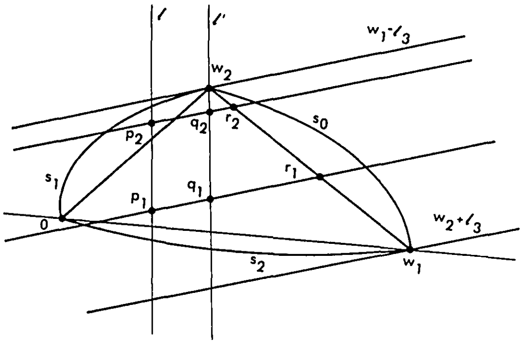

Fig. 19. Illustration of the proof that $p_1 - p_2 \in A$ when the line l intersects the arc s_1 and $p_1 - p_2$ is in the cone C_2.

APPENDIX C. PROOF THAT $B \sim S$ FOR CERTAIN POINTLIKE SETS

In this appendix we take the approach of first proving Theorem 1.

Theorem 1

If S satisfies Condition 2, then S is equivalent to a subset of B.

Then we prove Theorem 2.

Theorem 2

If S satisfies Conditions 2 and 3, then S is equivalent to B.

Finally we prove Theorem 3.

Theorem 3

Condition 1 is satisfied if and only if both Conditions 2 and 3 are satisfied.

It then follows from Theorems 2 and 3 that if S satisfies Condition 1 then S is equivalent to B.

Proof of Theorem 1

Let $G = \{0, w_1, w_2\}$. We have $0, w_1, w_2 \in A$. Since A is symmetric, we also have $-w_1, -w_2 \in A$. Furthermore, since $w_2 \in w_1 + A$, we have $w_2 - w_1 \in A$ and $w_1 - w_2 \in A$. Therefore,

$$G - G = \{0, w_1, -w_1, w_2, -w_2, w_1 - w_2, w_2 - w_1\} \subseteq A.$$

Also, G has three members. Therefore, by Condition 2, there exists $\upsilon \in E^N$ such that $\upsilon + \beta G \subseteq S$, where $\beta = \pm 1$. It follows that $G \subseteq \beta(S - \upsilon)$. Let $S_1 = \beta(S - \upsilon)$. Then $G \subseteq S_1$. Also, $S \sim S_1$, and therefore $A = S_1 - S_1$. We want to show that $S_1 \subseteq B$.

Let $x \in S_1$. We have $0 \in G \subseteq S_1$. Therefore

$$x = x - 0 \in S_1 - S_1 = A. \tag{C1}$$

Also, $w_1 \in G \subseteq S_1$. Therefore $x - w_1 \in S_1 - S_1 = A$ and

$$x \in w_1 + A. \tag{C2}$$

Similarly,

$$x \in w_2 + A. \tag{C3}$$

From Eqs. (C1)–(C3), it follows that $x \in B$. Since x was an arbitrary element of S_1, it follows that $S_1 \subseteq B$.

Proof of Theorem 2

Let υ, β, and S_1 be defined as in the proof of Theorem 1. Then, by that same proof, $S_1 \subseteq B$. We want to show that $B \subseteq S_1$. Let $x \in B$. We want to show that $x \in S_1$.

First, suppose that $x \in G$. Then, since $G \subseteq S_1$, $x \in S_1$, and we are done. Now assume that $x \notin G$. Let

$$G_i = \{0, x, w_i\}, \qquad i = 1, 2.$$

Since $x \in B$, it follows that $x \in A$ and $-x \in A$. We also have $w_i \in A$ and $-w_i \in A$. Furthermore, since $x \in w_i + A$, $x - w_1 \in A$, and $w_i - x \in A$. Therefore

$$G_i - G_i = \{0, x, -x, w_i, -w_i, x - w_i, w_i - x\} \subseteq A.$$

Also, G_i has three members. Therefore, by Condition 2, there exists $\upsilon_i \in E^N$ such that $\upsilon_i + \beta_i G_i \subseteq S$, where $\beta_i = \pm 1$.

Claim: There Exists $j \in \{1, 2\}$ such that $\beta_j = \beta$

Suppose not. Then $\beta_1 = \beta_2 = -\beta$. We have

$$\{\upsilon, \upsilon + \beta w_1, \upsilon + \beta w_2\} = \upsilon + \beta G \subseteq S$$

and

$$\{\upsilon_i, \upsilon_i + \beta_i x, \upsilon_i + \beta_i w_i\} = \upsilon_i + \beta_i G_i \subseteq \mathrm{S}, \qquad i = 1, 2.$$

Also, since $\beta_1 = \beta_2 = -\beta$,

$$(\upsilon + \beta w_i) - \upsilon = \upsilon_i - (\upsilon_i + \beta_i w_i), \qquad i = 1, 2.$$

Now, applying Condition 3, with

$$x_1 = \upsilon + \beta w_i, \qquad x_2 = \upsilon, \qquad y_1 = \upsilon_i, \qquad y_2 = \upsilon_i + \beta_i w_i,$$

we conclude that

$$\upsilon_i = \upsilon + \beta w_i, \qquad i = 1, 2. \tag{C4}$$

Furthermore,

$$\upsilon_1 - (\upsilon_1 + \beta_1 x) = \upsilon_2 - (\upsilon_2 + \beta_2 x).$$

It therefore follows from Condition 3 that

$$\upsilon_1 = \upsilon_2. \tag{C5}$$

From Eqs. (C4) and (C5) it follows that $w_1 = w_2$. This contradicts the assumption that $w_1 \neq w_2$ and proves the claim that there exists $j \in \{1, 2\}$ such that $\beta_j = \beta$.

Now we have

$$(\upsilon_j + \beta_j w_j) - \upsilon_j = (\upsilon + \beta w_j) - \upsilon.$$

By Condition 3, $\upsilon_j = \upsilon$. Therefore

$$\upsilon + \beta x = \upsilon_j + \beta_j x \in \upsilon_j + \beta_j G_j \subseteq S$$

and

$$x \in \beta(S - \upsilon) = S_1.$$

Proof of Theorem 3

Part 1: $1 \rightarrow 2$

Let G have three elements, $0 \in G \subseteq A$, and $G - G \in A$. We want to show that G is equivalent to a subset of S. That is, we want to show that there exists $\upsilon \in E^N$ such that $\upsilon + \beta G \in S$, where $\beta = \pm 1$.

Let $G = \{0, g_1, g_2\}$. Then $0 \neq g_1 \neq g_2 \neq 0$ and

$$\{0, g_1, -g_1, g_2, -g_2, g_1 - g_2, g_2 - g_1\} = G - G \subseteq A.$$

Since $A = S - S$, there exists $x_1, x_2, y_1, y_2, z_1, z_2 \in S$ such that $g_1 = x_1 - x_2$, $g_2 - g_1 = y_1 - y_2$, and $-g_2 = z_1 - z_2$. Then $x_1 \neq x_2$ and

$$x_1 - x_2 + y_1 - y_2 + z_1 - z_2 = 0. \quad \text{(C6)}$$

Therefore, by Condition 1,

$$x_1 = y_2 \quad \text{or} \quad x_1 = z_2, \quad \text{and} \quad x_2 = y_1 \quad \text{or} \quad x_2 = z_1.$$

Claim 1: One Cannot Have $x_1 = y_2$ *and* $x_2 = y_1$
If this were the case, then it would follow from Eq. (C6) that $z_1 - z_2 = 0$. But $z_1 - z_2 = -g_2 \neq 0$. This proves Claim 1.

Claim 2: One Cannot Have $x_1 = z_2$ *and* $x_2 = z_1$
If this were the case, then it would follow from Eq. (C6) that $y_1 - y_2 = 0$. But $y_1 - y_2 = g_2 - g_1 \neq 0$. This proves Claim 2.

Therefore either $x_1 = y_2$ and $x_2 = z_1$, or $x_1 = z_2$ and $x_2 = y_1$.

Case 1: $x_1 = y_2$ *and* $x_2 = z_1$
We have

$$y_1 - x_2 = x_1 - x_2 + y_1 - y_2 = g_1 + g_2 - g_1 = g_2$$

and $x_1 - x_2 = g_1$. Rewriting these equations, we have $x_2 + g_2 = y_1$ and $x_2 + g_1 = x_1$. Therefore

$$x_2 + G = \{x_2, x_2 + g_1, x_2 + g_2\} = \{x_2, x_1, y_1\} \subseteq S.$$

Letting $v = x_2$ and $\beta = 1$, we have $v + \beta G \subseteq S$.

Case 2: $x_1 = z_2$ *and* $x_2 = y_1$
We have

$$z_1 - x_2 = x_1 - x_2 + z_1 - z_2 = g_1 - g_2$$

and $x_1 - x_2 = g_1$. This yields $z_1 = x_2 + g_1 - g_2$ and $x_1 = x_2 + g_1$. Therefore

$$x_2 + g_1 - G = \{x_2 + g_1, x_2, x_2 + g_1 - g_2\} = \{x_1, x_2, z_1\} \subseteq S.$$

Letting $v = x_2 + g_1$ and $\beta = -1$, we have $v + \beta G \subseteq S$.

Part 2: $1 \rightarrow 3$
Let $u_1, u_2, v_1, v_2 \in S$, with $u_1 \neq u_2$ and $u_1 - u_2 = v_1 - v_2$. We want to show that $u_1 = v_1$. Let

$$x_1 = v_2, \quad x_2 = v_1, \quad y_1 = v_1, \quad y_2 = u_2,$$
$$z_1 = u_1, \quad z_2 = v_1.$$

Then $x_1 \neq x_2$ and

$$x_1 - x_2 + y_1 - y_2 + z_1 - z_2 = 0. \quad \text{(C7)}$$

Therefore, by Condition 1, $x_1 = y_2$ or $x_1 = z_2$, and $x_2 = y_1$ or $x_2 = z_1$. Now

$$z_2 - x_1 = v_1 - v_2 = u_1 - u_2 \neq 0.$$

Therefore, $x_1 \neq z_2$ and hence $x_1 = y_2$, or $v_2 = u_2$. Since, by assumption, $u_1 - u_2 = v_1 - v_2$, it follows that $u_1 = v_1$. This completes Part 2 of the proof.

Part 3: 2 and $3 \rightarrow 1$
Let $x_1, x_2, y_1, y_2, z_1, z_2 \in S$, with $x_1 \neq x_2$

and

$$x_1 - x_2 + y_1 - y_2 + z_1 - z_2 = 0. \quad \text{(C8)}$$

We want to show that $x_1 = y_2$ or $x_1 = z_2$, and $x_2 = y_1$ or $x_2 = z_1$.

Case 1: $y_1 = y_2$
In this case, it follows from Eq. (C8) that

$$x_1 - x_2 = z_2 - z_1. \quad \text{(C9)}$$

Therefore, by Condition 3, $x_1 = z_2$, and it follows from Eq. (C9) that $x_2 = z_1$.

Case 2: $z_1 = z_2$
Here, it follows from Eq. (C8) that

$$x_1 - x_2 = y_2 - y_1. \quad \text{(C10)}$$

Then, by Condition 3, $x_1 = y_2$, and it follows from Eq. (C10) that $x_2 = y_1$.

Case 3: $y_1 \neq y_2$ *and* $z_1 \neq z_2$
Let $g_1 = x_1 - x_2$ and $g_2 = y_2 - y_1$, and let $G = \{0, g_1, g_2\}$. Now, $g_1, g_2 \in S - S = A$, and hence also $-g_1, -g_2 \in A$. Furthermore,

$$g_1 - g_2 = x_1 - x_2 + y_1 - y_2 = z_2 - z_1 \in S - S = A,$$

and hence also $g_2 - g_1 \in A$. Thus we have $0 \in G \subseteq A$ and $G - G \subseteq A$. We also have $g_1 = x_1 - x_2 \neq 0$, $g_2 = y_2 - y_1 \neq 0$, and $g_1 - g_2 = z_2 - z_1 \neq 0$. Therefore G has three members. Hence, by Condition 2, there exists $v \in E^N$ such that $v + \beta G \subseteq S$, where $\beta = \pm 1$.

Subcase 3a: $\beta = 1$
We have

$$\{v, v + g_1, v + g_2\} = v + \beta G \subseteq S. \quad \text{(C11)}$$

Now, $(v + g_1) - v = g_1 = x_1 - x_2$. Therefore, by Condition 3, $v = x_2$, and hence, by Eq. (C11), $x_2 + g_1 \in S$ and $x_2 + g_2 \in S$. Now $(x_2 + g_2) - x_2 = g_2 = y_2 - y_1$. Therefore, by Condition 3, $x_2 + g_2 = y_2$ and $x_2 = y_1$. Also

$$(x_2 + g_1) - (x_2 + g_2) = g_1 - g_2 = z_2 - z_1.$$

Therefore, by Condition 3, $x_2 + g_1 = z_2$. But $x_2 + g_1 = x_1$. Therefore $x_1 = z_2$.

Subcase 3B; $\beta = -1$
We have

$$\{v, v - g_1, v - g_2\} = v + \beta G \subseteq S. \quad \text{(C12)}$$

Now $v - (v - g_1) = g_1 = x_1 - x_2$. Therefore, by Condition 3, $v = x_1$, and hence, by Eq. (C12), $x_1 - g_1 \in S$ and $x_1 - g_2 \in S$. Now $x_1 - (x_1 - g_2) = g_2 = y_2 - y_1$. Therefore, by Condition 3, $x_1 = y_2$. Also,

$$(x_1 - g_1) - (x_1 - g_2) = g_2 - g_1 = z_1 - z_2.$$

Therefore, by Condition 3, $x_1 - g_1 = z_1$. But $x_1 - g_1 = x_2$. Therefore $x_2 = z_1$.

ACKNOWLEDGMENT

This research was supported by the U.S. Air Force Office of Scientific Research under contract no. F49620-80-C-0006.

* Present address, Martin Marietta Aerospace, Orlando Division, M.P. 304, P.O. Box 5837, Orlando, Florida 32855.

REFERENCES

1. See, for example, H. P. Baltes, ed., *Inverse Source Problems in Optics* (Springer-Verlag, New York, 1978).
2. J. R. Fienup, "Reconstruction of an object from the modulus of its Fourier transform," Opt. Lett. 3, 27–29 (1978); "Space object imaging through the turbulent atmosphere," Opt. Eng. 18, 529–534 (1979).
3. R. N. Bracewell, *The Fourier Transform and Its Applications*, 2nd ed. (McGraw-Hill, New York, 1978).
4. H. W. E. Jung, "Uber die kleinste Kugel, die eine raumliche Figur einschliesst," Z. Reine Agnew. Math. **123,** 241 (1901).
5. J. Christou, "Imaging of star clusters from speckle interferometry," Opt. Commun. **37**, 331–334 (1981).
6. J. R. Fienup and T. R. Crimmins, "Determining the support of an object from the support of its autocorrelation," J. Opt. Soc. Am. **70**, 1581(A) (1980).