Uniqueness of phase retrieval for functions with sufficiently disconnected support

T. R. Crimmins and J. R. Fienup

Environmental Research Institute of Michigan, P.O. Box 8618, Ann Arbor, Michigan 48107

Received August 24, 1982

It is shown that the phase-retrieval problem almost always has a solution unique among functions with disconnected supports satisfying a certain common separation condition.

INTRODUCTION

The problem of phase retrieval is to reconstruct a function $f(x)$ from the modulus $|F(u)|$ of its Fourier transform,

$$F(u) = \int_{-\infty}^{\infty} f(x)e^{-iux}\mathrm{d}x.$$

This is equivalent to reconstructing the phase of $F(u)$ from $|F(u)|$ or to reconstructing $f(x)$ from its autocorrelation function, which is given by the inverse Fourier transform of $|F(u)|^2$. This problem arises in many fields, including astronomy, x-ray crystallography, wave-front sensing, pupil-function determination, electron microscopy, and particle scattering. In this paper the function f is assumed to be a square-integrable, one-dimensional, complex-valued function.

In the most general case, many different functions have the same Fourier modulus. A solution can be obtained simply by multiplying $|F|$ by any measurable complex-valued function with modulus one and taking the inverse Fourier transform.

When f has compact support (i.e., f is zero outside some finite interval), the degree of ambiguity is reduced, but there still may be (and usually are) many other solutions that also have compact support. Hofstetter[1] and Walther[2] showed that all solutions with compact support could be obtained from any one of them by flipping (conjugating) nonreal zeros of its Fourier transform extended by analyticity to the complex plane (i.e., the Laplace transform).

Greenaway[3] showed that, if F has only a finite number of nonreal zeros and if f has disconnected support contained in the union of two disjoint intervals, then it is almost always essentially the only solution with support contained in the union of those two intervals. The meaning of the terms "almost always" and "essentially" used here are explained later. Bates[4] also discussed the uniqueness of functions with disconnected support.

Crimmins and Fienup[5] showed, by a counterexample, that Greenaway's result is not true if F has an infinite number of nonreal zeros. This creates a problem because it has been shown[6] that functions whose Laplace transforms have only a finite number of nonreal zeros satisfy certain special conditions. Thus the Laplace transforms of most functions gotten more or less randomly from the real world will have an infinite number of nonreal zeros, in which case Greenaway's analysis does not apply.

In this paper it is shown that, if f has disconnected support contained in the union of a sequence of intervals satisfying a certain separation condition, then f is almost always essentially the only solution with support contained in the union of those intervals. This holds no matter how many nonreal zeros F has.

EQUIVALENT SOLUTIONS

Let c be a real number and C be a complex number, with $|C| = 1$, and let $g(x) = Cf(x + c)$ and $h(x) = \overline{Cf(-x + c)}$, where the overbar denotes complex conjugation. If F, G, and H are the Fourier transforms of f, g, and h, respectively, then

$$G(u) = Ce^{icu}F(u), \qquad H(u) = \overline{Ce^{-icu}F(u)}.$$

Thus

$$|G(u)| = |F(u)| = |H(u)|.$$

The solutions f, g, and h are called *equivalent* or, in symbols,

$$g \approx f \approx h.$$

If all solutions are equivalent to f, then f is said to be *essentially* the only solution or the *unique* solution.

THE THEOREM

Let I_n, $n = 1, \ldots, N$ be a sequence of nonoverlapping closed intervals. Define

$$I_m - I_n = \{x - y: x \in I_m, y \in I_n\}.$$

We will assume that the following condition is satisfied.

Separation Condition: $(I_m - I_n) \cap (I_j - I_k) = \phi$ for $1 \leq m, n, j, k \leq N$; $j \neq k$; and $(m, n) \neq (j, k)$, where (,) denotes an ordered pair. (Note that $m = n$ is allowed in the above condition.)

For $N = 2$, this condition is equivalent to the requirement that the lengths of the two intervals be less than the distance between them. For an example of three intervals satisfying

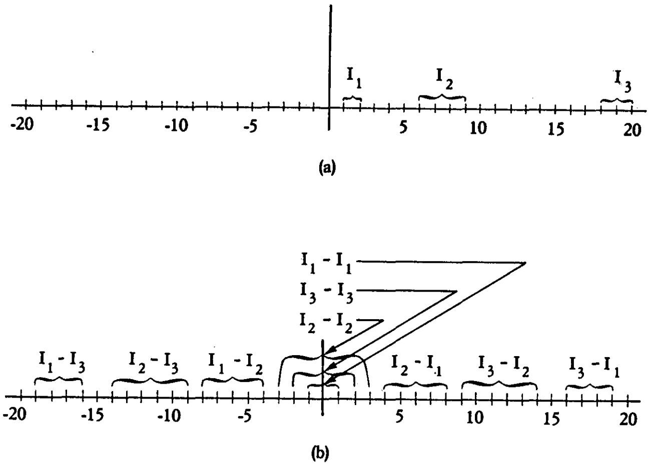

Fig. 1. (a) Example of three intervals satisfying the separation condition, (b) the autocorrelation intervals $I_n - I_m$.

the separation condition, let

$$I_1 = [1, 2], \qquad I_2 = [6, 9], \qquad I_3 = [18, 20],$$

as shown in Fig. 1(a). Then, as shown in Fig. 1(b),

$$\begin{aligned} I_1 - I_1 &= [-1, 1], \\ I_2 - I_2 &= [-3, 3], \\ I_3 - I_3 &= [-2, 2], \\ I_2 - I_1 &= [4, 8], \\ I_1 - I_2 &= [-8, -4], \\ I_3 - I_2 &= [9, 14], \\ I_2 - I_3 &= [-14, -9], \\ I_3 - I_1 &= [16, 19], \\ I_1 - I_3 &= [-19, -16]. \end{aligned}$$

Returning to the general case, let

$$A = \bigcup_{n=1}^{N} I_n,$$

and let f and g be two complex-valued square-integrable functions, both of which are zero outside A. For $n = 1, \ldots, N$, let

$$f_n(x) = \begin{cases} f(x), & \text{for } x \in I_n \\ 0, & \text{otherwise} \end{cases}$$

and

$$g_n(x) = \begin{cases} g(x), & \text{for } x \in I_n \\ 0, & \text{otherwise} \end{cases}.$$

Then

$$f(x) = \sum_{n=1}^{N} f_n(x), \qquad g(x) = \sum_{n=1}^{N} g_n(x).$$

It is assumed that $f_n \not\equiv 0$ [i.e., $f_n(x)$ is not identically zero], $n = 1, \ldots, N$.

Note that the autocorrelation of $f(x)$ can be expressed as the sum of N^2 cross-correlation terms,

$$f(x) * \tilde{f}(x) = \sum_{m=1}^{N} \sum_{n=1}^{N} f_m(x) * \tilde{f}_n(x),$$

where $*$ denotes convolution and

$$\tilde{f}(x) = \overline{f(-x)}.$$

The cross-correlation term $f_m(x) * \tilde{f}_n(x)$ has support contained within $I_m - I_n$. Of these N^2 terms, N of them have $m = n$ and are centered at the origin. The remaining $N^2 - N$ cross-correlation terms, for which $m \neq n$, are centered elsewhere. The separation condition is equivalent to requiring that none of those $N^2 - N$ cross-correlation terms overlaps with another or with the terms centered at the origin.

Let F, G, F_n, and G_n be the Laplace transforms of f, g, f_n, and g_n, respectively. Let $Z(F)$ be the set of nonreal zeros of F, and define $Z(G)$, $Z(F_n)$, and $Z(G_n)$ similarly.

Let

$$B = \bigcap_{n=1}^{N} Z(F_n),$$

that is, B is the set of nonreal zeros common to all the F_n. Finally, let $w = u + iv$ be a variable in the complex plane, and define

$$F^*(w) = \overline{F(\overline{w})}.$$

The functions G^*, F_n^*, and G_n^* are defined similarly.

Theorem: If the supports of f and g satisfy the same separation condition defined above and $f_n \not\equiv 0$, $n = 1, \ldots, N$, and if $|F(u)| = |G(u)|$ for all real numbers u, then there exist a real number c, a complex number C with $|C| = 1$, and a strictly positive integer-valued function α defined on a set $B_0 \subseteq B$, such that for $N \neq 2$

$$G_n(w) = Ce^{icw}\Phi(w)F_n(w), \qquad n = 1, \ldots, N \qquad \text{(a)}$$

and for $N = 2$ either (a) holds or

$$\begin{aligned} G_1^*(w) &= Ce^{icw}\Phi(w)F_2(w), \\ G_2^*(w) &= Ce^{icw}\Phi(w)F_1(w), \end{aligned} \qquad \text{(b)}$$

where

$$\Phi(w) = \prod_{z \in B_0} \left(\frac{1 - \dfrac{w}{\overline{z}}}{1 - \dfrac{w}{z}} \right)^{\alpha(z)}$$

The integer $\alpha(z)$ determines how many zeros at location z are being flipped. The proof of this theorem is given in Appendix A.

If $B = \phi$, i.e., there are no nonreal zeros common to all the F_n, then $\Phi \equiv 1$, and conclusion (a) of the theorem becomes

$$G_n(w) = Ce^{icw}F_n(w), \qquad n = 1, \ldots, N \qquad \text{(a}')$$

and conclusion (b) becomes

$$G_1^*(w) = Ce^{icw}F_2(w), \qquad G_2^*(w) = Ce^{icw}F_1(w). \qquad (b')$$

In either case if follows that $f \approx g$ if $B = \phi$. This proves the following corollary.

Corollary: If $B = \phi$ and $|F(u)| = |G(u)|$ for all real numbers u, then $f \approx g$.

We note that, since $|F(u)|^2$ and $|G(u)|^2$ are analytic functions, the condition that $|F(u)| = |G(u)|$ for all real u is implied by the condition that this equality hold for all u in some open interval.

CONCLUSIONS

If f has $N \geq 2$ separated parts contained within a set A satisfying the separation condition and f is gotton more or less randomly from the real world, then the set B will almost always be null. That is, it is unlikely that the Laplace transforms of the separated parts of f will have nonreal zeros common to all the parts. Thus we may conclude in this case of functions with sufficiently separated parts that the phase-retrieval problem almost always has a unique solution among functions having support contained within A.

Note, however, that our earlier counterexample[5] demonstrates that, even when the separation condition is satisfied for f and $B = \phi$, there can be nonequivalent solutions having supports not contained in the set A. Only by specifying a stronger separation condition and requiring f to be real and nonnegative can one ensure that f is unique among all nonnegative functions of compact support. Specifically, it can be shown[6] for $N = 2$ that if $[-d, d]$ is the smallest closed interval containing the support of the autocorrelation of f, which support is also contained within $[-d, -d/2] \cup (-d/3, d/3) \cup [d/2, d]$, and if $B = \phi$, then f is unique among nonnegative functions.

It should also be noted that, since a two-dimensional analog of the zero-flipping theorem of Hofstetter and Walther does not now exist, these results do not automatically extend to the two-dimensional case. However, from other considerations, both theoretical[7] and experimental,[8] it appears that the probability of uniqueness is high for two-dimensional functions of compact support, even when the support is not disconnected.

APPENDIX A. PROOF OF THE THEOREM:

Case 1: $N \neq 2$

Define $\tilde{f}(x) = \overline{f(-x)}$. Then $f * \tilde{f}$ (where $*$ denotes convolution) is the autocorrelation of f. Since the Fourier transform of the autocorrelation of f is $|F(u)|^2 = |G(u)|^2$, it follows that

$$f(x) * \tilde{f}(x) = g(x) * \tilde{g}(x). \tag{1}$$

It follows from the separation condition that, for $n \neq m$,

$$f_n(x) * \tilde{f}_m(x) = \begin{cases} f(x) * \tilde{f}(x), & \text{for } x \in I_n - I_m \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

and

$$g_n(x) * g_m(x) = \begin{cases} g(x) * \tilde{g}(x), & \text{for } x \in I_n - I_m \\ 0, & \text{otherwise} \end{cases}. \tag{3}$$

It then follows from Eqs. (1–3) that

$$f_n(x) * \tilde{f}_m(x) = g_n(x) * \tilde{g}_m(x) \qquad \text{for } n \neq m. \tag{4}$$

Since the Laplace transforms of $\tilde{f}_n$ and $\tilde{g}_n$ are F_n^* and G_n^*, respectively, it follows from Eq. (4) that

$$F_n F_m^* = G_n G_m^* \qquad \text{for } n \neq m. \tag{5}$$

If $N \geq 3$, let n_1, n_2, and n_3 be three distinct integers ≥ 1 and $\leq N$. Then

$$F_{n_1} F_{n2}^* F_{n2} F_{n3}^* = G_{n_1} G_{n2}^* G_{n_2} G_{n3}^* \tag{6}$$

and

$$F_{n_1} F_{n3}^* = G_{n_1} G_{n3}^*. \tag{7}$$

Since it was assumed the $f_n \not\equiv 0$, it follows that $F_n \not\equiv 0$, $n = 1, \ldots, N$. Since all the functions appearing in Eqs. (6) and (7) are also entire, we may divide Eq. (6) by Eq. (7) and obtain

$$F_{n2}^* F_{n2} = G_{n2}^* G_{n2}.$$

Therefore, if $N \geq 3$,

$$F_n F_n^* = G_n G_n^*, \qquad n = 1, \ldots, N. \tag{8}$$

Equations (8) hold also for $N = 1$ since $FF^* = GG^*$ and, in this case, $F_1 = F$ and $G_1 = G$. Combining Eqs. (5) and (8),

$$F_n F_m^* = G_n G_m^* \qquad \text{for } n, m = 1, \ldots, N. \tag{9}$$

It follows from Eqs. (8) and the zero-flipping theorem proved by Hofstetter[1] and Walther[2] that, for each n, $1 \leq n \leq N$, there exists a set $B_n \subseteq Z(F_n)$ and a strictly positive integer-valued function α_n, defined on B_n, and a real number c_n and a complex number C_n, with $|C_n| = 1$, such that

$$G_n(w) = C_n \exp(ic_n w) \Phi_n(w) F_n(w), \tag{10}$$

where

$$\Phi_n(w) = \prod_{z \in B_n} \left(\frac{1 - \dfrac{w}{\bar{z}}}{1 - \dfrac{w}{z}} \right)^{\alpha_n(z)}. \tag{11}$$

It follows from Eq. (10) that

$$G_n^*(w) = \overline{C}_n \exp(-ic_n w) \Phi_n^*(w) F_n^*(w). \tag{12}$$

Now,

$$\Phi_n^*(w) = \prod_{z \in B_n} \left(\frac{1 - \dfrac{w}{z}}{1 - \dfrac{w}{\bar{z}}} \right)^{\alpha_n(z)},$$

and therefore

$$\Phi_n \Phi_n^* \equiv 1, n = 1, \ldots, N. \tag{13}$$

From Eqs. (9), (10), and (12), for $n, m = 1, \ldots, N$,

$$\begin{aligned} F_n(w) F_m^*(w) &= G_n(w) G_m^*(w) \\ &= C_n \overline{C}_m \exp[i(c_n - c_m)w] \Phi_n(w) \Phi_m^*(w) F_n(w) F_m^*(w). \end{aligned}$$

Thus

$$1 = C_n \overline{C}_m \exp[i(c_n - c_m)w] \Phi_n(w) \Phi_m^*(w),$$

and, by Eq. (13),

$$C_m \exp(ic_m w) \Phi_m(w) = C_n \exp(ic_n w) \Phi_n(w). \tag{14}$$

Since the exponential functions appearing in Eq. (14) have no zeros or poles, it follows that the meromorphic functions Φ_n and Φ_m have the same zeros and poles of the same order. Therefore

$$B_n = B_m, \qquad \alpha_n = \alpha_m,$$

and hence

$$\Phi_n = \Phi_m, \qquad n, m = 1, \ldots, N.$$

Let

$$B_o = B_n, \qquad \alpha = \alpha_n, \qquad \Phi = \Phi_n, \qquad n = 1, \ldots, N.$$

Then, since

$$B_o = B_n \subseteq Z(F_n), \qquad n = 1, \ldots, N,$$

it follows that

$$B_o \subseteq B.$$

Also, from Eq. (14),

$$C_n \exp(ic_n w) = C_m \exp(ic_m w),$$

from which it follows that

$$C_n = C_m, \qquad c_n = c_m, \qquad n, m = 1, \ldots, N.$$

Let

$$C = C_n, \qquad c = c_n, \qquad n = 1, \ldots, N.$$

Then, from Eq. (10),

$$G_n(w) = Ce^{icw}\Phi(w)F_n(w), \qquad n = 1, \ldots, N.$$

This completes the proof for Case I.

Case II: $N = 2$

Let

$$I = (I_1 - I_1) \cup (I_2 - I_2).$$

It follows from the separation condition that

$$I \cap (I_n - I_m) = \phi \qquad \text{for } n \neq m,$$

and $F_1F_1^* + F_2F_2^*$ is the restriction of FF^* to I and $G_1G_1^* + G_2G_2^*$ is the restriction of GG^* to I. Therefore, since $FF^* = GG^*$,

$$F_1F_1^* + F_2F_2^* = G_1G_1^* + G_2G_2^*. \tag{15}$$

As before, we also have

$$F_1F_2^* = G_1G_2^*, \qquad F_1^*F_2 = G_1^*G_2. \tag{16}$$

From Eqs. (15) and (16), we obtain

$$\begin{aligned}(F_1F_1^* - G_1G_1^*)(F_1F_1^* - G_2G_2^*) &= (F_1F_1^*)^2 - (G_1G_1^* + G_2G_2^*)F_1F_1^* + (G_1G_2^*)(G_1^*G_2)\\ &= (F_1F_1^*)^2 - (F_1F_1^* + F_2F_2^*)F_1F_1^* + (F_1F_2^*)(F_1^*F_2)\\ &= 0.\end{aligned}$$

Therefore, since all functions involved are entire, either

$$F_1F_1^* = G_1G_1^* \tag{17a}$$

and, by Eq. (15),

$$F_2F_2^* = G_2G_2^* \tag{17b}$$

or

$$F_1F_1^* = G_2G_2^* \tag{18a}$$

and, by Eq. (15),

$$F_2F_2^* = G_1G_1^*. \tag{18b}$$

If Eqs. (17) hold, then the same argument used in the case $N \neq 2$ applies, and conclusion (a) of the theorem follows. If Eqs. (18) hold, let

$$H_1 = G_2^*, \qquad H_2 = G_1^*, \qquad H = H_1 + H_2.$$

Then

$$H_1H_1^* = F_1F_1^*, \qquad H_2H_2^* = F_2F_2^*,$$
$$H_1H_2^* = F_1F_2^*, \qquad H_1H_2^* = F_1F_2^*,$$

and

$$HH^* = FF^*.$$

Therefore the argument used in case $N \neq 2$ applies with G, G_1, and G_2 replaced with H, H_1, and H_2, respectively, and conclusion (b) of the theorem follows. This completes the proof.

ACKNOWLEDGMENT

This research was supported by the U.S. Air Force Office of Scientific Research.

REFERENCES

1. E. M. Hofstetter, "Construction of time-limited functions with specified autocorrelation functions," IEEE Trans. Inf. Theory **IT-10,** 119–126 (1964).
2. A. Walther, "The question of phase retrieval in optics," Opt. Acta **10,** 41–49 (1963).
3. A. H. Greenaway, "Proposal for phase recovery from a single intensity distribution," Opt. Lett. **1,** 10–12 (1977).
4. R. H. T. Bates, "Fringe visibility intensities may uniquely define brightness distributions," Astron. Astrophys. **70,** L27–L29 (1978).
5. T. R. Crimmins and J. R. Fienup, "Ambiguity of phase retrieval for functions with disconnected support," J. Opt. Soc. Am. **71,** 1026–1028 (1981).
6. T. R. Crimmins and J. R. Fienup, "Phase retrieval for functions with disconnected support," in App. B of J. R. Fienup, "High resolution imaging of space objects," interim scientific report to U.S. Air Force Office of Scientific Research, ERIM Rep. No. 145400-7-P (Environmental Research Institute of Michigan, Ann Arbor, Mich., March 1981).
7. Yu. M. Bruck and L. G. Sodin, "On the ambiguity of the image reconstruction problem," Opt. Commun. **30,** 304–308 (1979).
8. J. R. Fienup, "Space object imaging through the turbulent atmosphere," Opt. Eng. **18,** 529–534 (1979).