$$= \frac{1}{2}\int_0^\infty \max_{w:\, w'v=1} h \exp\left(\frac{-h\Lambda_0(w)}{2\delta}\right) dh$$
$$= \frac{1}{2}\int_0^\infty h \exp\left(\frac{-h\Lambda(v)}{2\delta}\right) dh$$
$$= 2\delta^2 \Lambda(v)^{-2}$$

and the lemma is proven. □

The theorem now follows as a straightforward consequence of Lemma 7. If q_i is the ith standard unit vector, then

$$\|x - \hat{x}_k\|^2 = \sum_{i=1}^{r} |q_i'(x - \hat{x}_k)|^2.$$

Thus, Lemma 7 implies that

$$\liminf_{k\to\infty} k^2 \boldsymbol{E}\|x - \hat{x}_k\|^2 \geq 2\delta^2 \sum_{i=1}^{r} \Lambda(q_i)^{-2}.$$

ACKNOWLEDGMENT

S. Rangan would like to thank Prof. P. Khargonekar for his support during the completion of this work. The suggestions of Prof. M. Vetterli, an anonymous reviewer, and the associate editor are also gratefully acknowledged.

REFERENCES

[1] R. M. Gray, "Quantization noise spectra," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1220–1244, Nov. 1990.
[2] S. P. Lipshitz, R. A. Wannamaker, and J. Vanderkooy, "Quantization and dither: A theoretical survey," *J. Audio Eng. Soc.*, vol. 40, no. 5, pp. 355–375, May 1992.
[3] R. M. Gray and T. G. Stockham Jr., "Dithered quantizers," *IEEE Trans. Inform. Theory*, vol. 39, pp. 805–812, May 1993.
[4] L. Ljung, *Theory and Practice of Recursive Identification*. Cambridge, MA: MIT Press, 1983.
[5] S. S. Haykin, *Adaptive Filter Theory*, 3rd ed. Upper Saddle River, NJ: Prentice-Hall, 1996.
[6] N. T. Thao and M. Vetterli, "Reduction of the MSE in R-times oversampled A/D conversion from $O(1/R)$ to $O(1/R^2)$," *IEEE Trans. Signal Processing*, vol. 42, pp. 200–203, Jan. 1994.
[7] ——, "Deterministic analysis of oversampled A/D conversion and decoding improvement based on consistent estimates," *IEEE Trans. Signal Processing*, vol. 42, pp. 519–531, Mar. 1994.
[8] Z. Cvetković, "Overcomplete expansions for digital signal processing," Ph.D. dissertation, Univ. California, Berkeley, 1995.
[9] V. K. Goyal, M. Vetterli, and N. T. Thao, "Quantized overcomplete expansions in $\mathbb{R}^N$: Analysis, synthesis, and algorithms," *IEEE Trans. Inform. Theory*, vol. 44, pp. 16–31, Jan. 1998.
[10] N. T. Thao and M. Vetterli, "Lower bound on the mean-squared error in oversampled quantization of periodic signals using vector quantization analysis," *IEEE Trans. Inform. Theory*, vol. 42, pp. 469–479, Mar. 1996.
[11] Z. Cvetković, "Source coding with quantized redundant expansions: Accuracy and reconstruction," in *Proc. IEEE Data Compression Conf.*, J. A. Storer and M. Cohn, Eds. Snowbird, UT, Mar. 1999, pp. 344–353.
[12] R. Zamir and M. Feder, "Rate-distortion performance in coding bandlimited sources by sampling and dithered quantization," *IEEE Trans. Inform. Theory*, vol. 41, pp. 141–154, Jan. 1995.
[13] ——, "Information rates of pre/post-filtered dithered quantizers," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1340–1353, Sept. 1996.
[14] I. Daubechies, *Ten Lectures on Wavelets*. Philadelphia, PA: Soc. Industr. Appl. Math., 1992.
[15] M. Cwikel and P. O. Gutman, "Convergence of an algorithm to find maximal state constraint sets for discrete-time linear dynamical systems with bounded controls and states," *IEEE Trans. Automat. Contr.*, vol. AC-31, pp. 457–459, May 1986.
[16] M. Milanese and V. Vicino, "Optimal estimation theory for dynamic systems with set membership uncertainty: An overview," *Automatica*, vol. 27, no. 6, pp. 997–1009, Nov. 1991.
[17] H. J. Kushner and C. G. Lin, *Stochastic Approximation Algorithms and Applications*. New York: Springer-Verlag, 1997.
[18] J. Ziv and M. Zakai, "Some lower bounds on signal parameter estimation," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 386–391, May 1969.
[19] K. L. Bell, Y. Steinberg, Y. Ephraim, and H. L. Van Trees, "Extended Ziv–Zakai lower bound for vector parameter estimation," *IEEE Trans. Inform. Theory*, vol. 43, pp. 624–637, Mar. 1997.
[20] J. Ziv, "On universal quantization," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 344–347, May 1985.
[21] R. Zamir and M. Feder, "On universal quantization by randomized uniform/lattice quantization," *IEEE Trans. Inform. Theory*, vol. 38, pp. 428–436, Mar. 1992.
[22] Z. Cvetković and M. Vetterli, "Error-rate characteristics of oversampled analog-to-digital conversion," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1961–1964, Sept. 1998.
[23] M. J. Todd, "On minimum volume ellipsoids containing part of a given ellipsoid," *Math. Oper. Res.*, vol. 7, no. 2, pp. 253–261, May 1982.

Bounds for Sparse Planar and Volume Arrays

Yann Meurisse and Jean-Pierre Delmas, *Member, IEEE*

***Abstract*—This correspondence improves and extends bounds on the numbers of sensors, redundancies, and holes for sparse linear arrays to sparse planar and volume arrays. As an application, the efficiency of regular planar and volume arrays with redundancies but no holes is deduced. Also, examples of new redundancy and hole square arrays, found by exhaustive computer search, are given.**

***Index Terms*—Difference base, minimum hole array, minimum redundancy array, sparse planar array, sparse volume array.**

I. INTRODUCTION

When the number of antenna sensors available for an array is limited, the problem of optimum array geometry naturally arises. From the beam width and the sidelobe level of the associated beam pattern [1] or from the direction of arrival (DOA) estimation accuracy [2] point of view, array configurations known as linear minimum-redundancy (MR) arrays or linear minimum-hole (MH) arrays (also called optimum nonredundant arrays) are often proposed. Linear MR arrays have been extensively studied; see [3] and [4], and the references therein. In particular, much attention has been given to bounds on the ratio M^2/A [4], [5] where M and A denote, respectively, the number of sensors and the aperture of the linear array. Linear MH arrays were considered in [3] and [6]. Whereas specific structures were designed to optimize some performance criteria (e.g., [7] for DOA algorithms with DOA prior information and [1] for beam patterns with various sidelobe level/beamwidth tradeoffs); redundancy and hole concepts do not embrace any such optimality criterion directly. Thus, the MR and MH

Manuscript received June 30, 1999; revised June 22, 2000. The material in this correspondence was presented at the Millenium Conference on Anbtennas and Propagation AP2000, Davos, Switzerland, April 9–14, 2000.

The authors are with the Département Signal et Image, Institut National des Télécommunications, 91011 Evry Cedex, France (e-mail: yann.meurisse@int-evry.fr; jean-pierre.delmas@int-evry.fr).

Communicated by J. A. O'Sullivan, Associate Editor for Detection and Estimation.

Publisher Item Identifier S 0018-9448(01)00579-X.

TABLE I
NUMBERS OF SENSORS AND CONFIGURATIONS OF SQUARE MR (RESP., MH) ARRAYS OBTAINED BY EXHAUSTIVE COMPUTER SEARCH COMPARED WITH LOWER BOUND (LB) (RESP., UPPER BOUND (UB)), VERSUS APERTURE

Aperture	square MR array					square MH array		
	M_{min}	LB	Number of configurations			M_{max}	UB	Number of configurations
			Total	GW	CP			
2	7	6	2			5	5	1
3	9	8	4	1	1	6	7	36
4	12	10	4	1		8	8	4
5	15	13	83	1		9	10	347
6	16	15	≥ 1		1	11	12	1
7		17				12	14	113

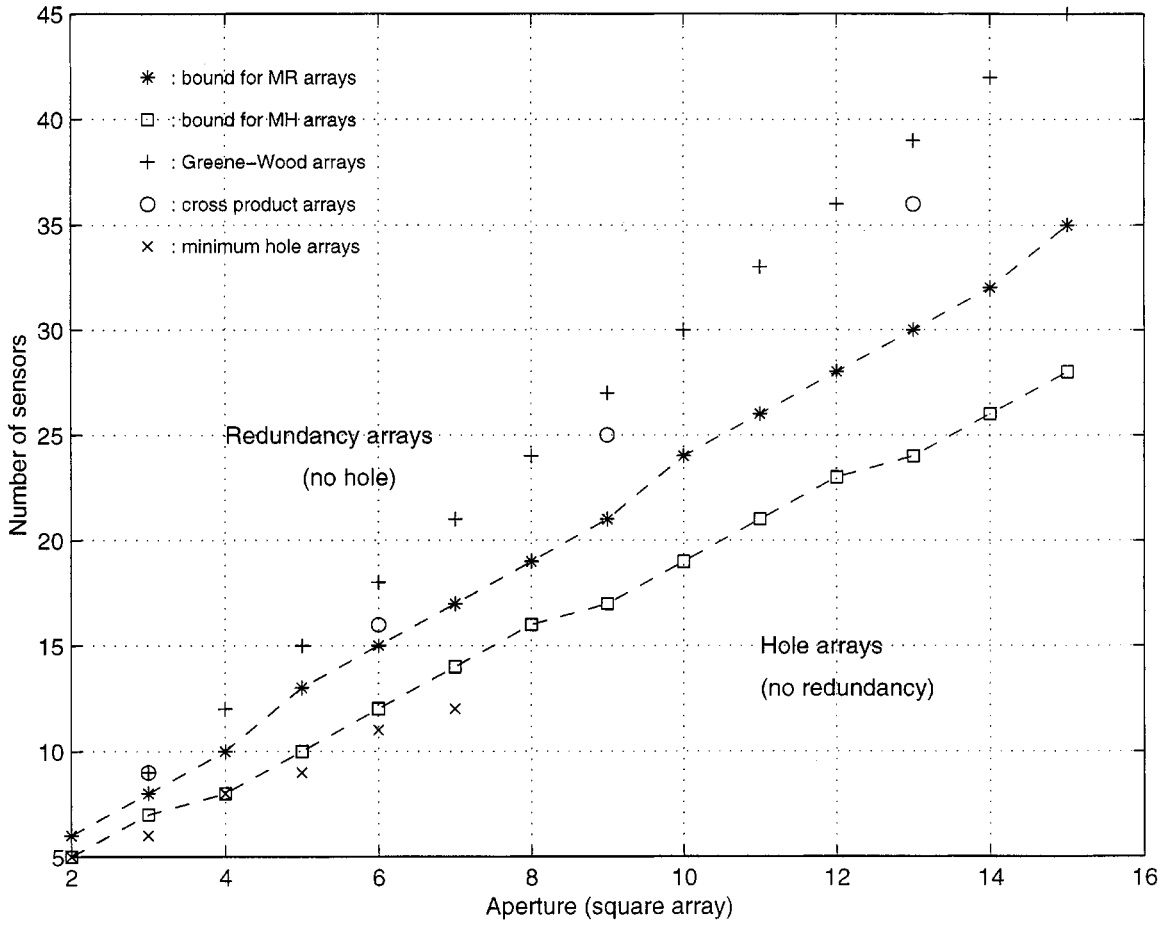

Fig. 1. Numbers of sensors (obtained by exhaustive computer search and bounds (2.5), (2.6) versus aperture of square array.

arrays are more easily applicable to a wider range of problems, and these structures achieve an efficient tradeoff between beam pattern and DOA estimation performance.

Contrary to the sparse linear arrays, few contributions have been devoted to sparse planar and volume arrays (note that the planar array retains side ambiguity resolved by a volume array). The notions of MR and MH arrays can be extended to these arrays because the spatial covariance matrix, associated with equally spaced arrays, exhibits a Toeplitz, block-Toeplitz structure for uncorrelated sources. Some structures of square and cubic redundancy arrays were studied by Pumphrey [8]. However, as discussed in [9], the computation of MR and MH arrays for the two-dimensional (2–D) case is much more involved than that for the one-dimensional (1–D) case. Thus, it is of importance to have bounds to be able to qualify the efficiency of not necessarily MR or MH planar and volume structures.

Section II improves and extends bounds on the numbers of sensors, redundancies, and holes for the sparse linear arrays given by [3] to sparse planar and volume arrays. As an application, the efficiency of regular planar and volume arrays with redundancies but no holes is deduced. Also, examples of new redundancy and hole square arrays given by exhaustive computer search are shown in the Appendix.

II. BOUNDS FOR ARRAYS WITH REDUNDANCIES AND HOLES

Consider a volume array $\mathcal{A}$ made of M sensors lying on the marks of a Cartesian grid.[1] The sensor spacings on this grid are integer multiples of some fundamental distance (usually the half wavelength of the

[1]It is possible to consider other kind of grid as Haubrich [10] did, who considered sensors on an isometric or equilateral triangle grid and found perfect planar arrays in this way.

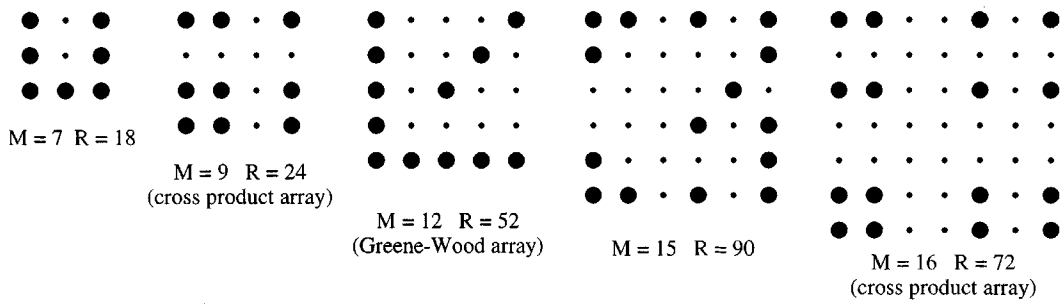

Fig. 2. Examples of square MR arrays.

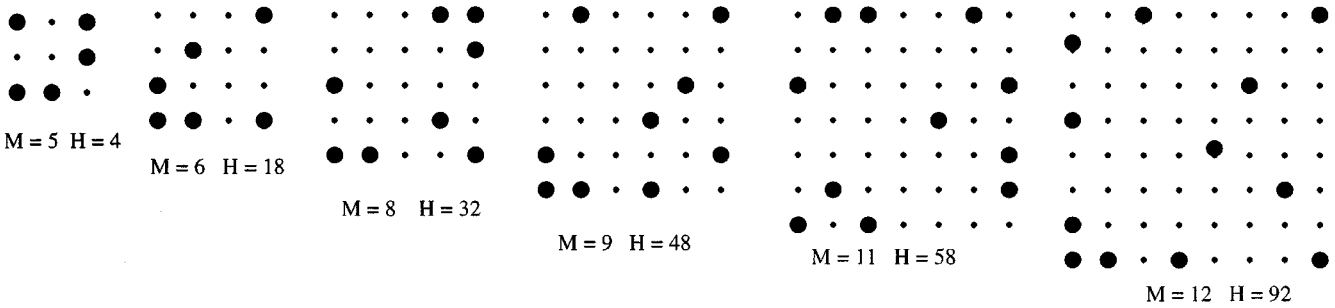

Fig. 3. Examples of square MH arrays.

incident radiation), and thus the sensor separations can be represented by these integers. Based on the assumption that one is primarily interested in how an array samples the spatial covariance function, which is a function only of the separation between the points (for uncorrelated sources), the useful notion of coarray was introduced [10]. It refers to the set of points at which the spatial covariance function can be estimated with that array. This coarray $\mathcal{D}$ is represented with a set of vectors $\boldsymbol{d}$ called lags

$$\mathcal{D} = \{\boldsymbol{d}_{ij} = \boldsymbol{s}_i - \boldsymbol{s}_j\}, \qquad i, j = 1, 2, \ldots, M$$

where $\boldsymbol{s}_i = (x_i, y_i, z_i)^T$ is the location of the ith sensor (x_i, y_i, and z_i are integers). Denote by

$$(A_x, A_y, A_z) = (\max(x_i - x_j), \max(y_i - y_j), \max(z_i - z_j))$$

the apertures of this array. Linear and planar arrays are considered as particular cases of volume arrays, i.e., $A_y = A_z = 0$ and $A_z = 0$ for, respectively, linear and planar arrays. With these definitions, we recall that if the array has more than one pair of sensors separated by the same lag $\boldsymbol{d}$, these pairs produce redundant estimates of the covariance function at that lag. In this case, the coarray of that array is said to have redundancies. The number of these redundancies excluding the lag $\mathbf{0}$ is denoted by R. If there is no pair of sensors separated by some lag whose components are all smaller than the associated apertures of the array, the array is said to have a hole in its coarray at that location. The number of these holes is denoted by H. If E is the number of distinct lags of the coarray (including lag $\mathbf{0}$), the number M^2 of lags $\boldsymbol{d}_{ij}$ of the coarray is composed of E lags appearing at least one time and of $R + M - 1$ strictly redundant lags, so $M^2 = E + R + (M - 1)$. Each of the $(2A_x + 1)(2A_y + 1)(2A_z + 1)$ lags of the rectangular parallelepiped associated full array appears either at least one time or not at all, so $E+H = (2A_x+1)(2A_y+1)(2A_z+1)$. Consequently, the apertures, the numbers of sensors, redundancies, and holes are related by

$$(2A_x + 1)(2A_y + 1)(2A_z + 1) = (M^2 - M + 1) + H - R. \quad (2.1)$$

To eliminate the apertures in this relation and derive a general relation between the numbers of sensors, redundancies, and holes, we introduce a new function associated with its autocorrelation function that enables us to improve and to extend directly the linear array bounds by [3] to planar and volume arrays. Let $\chi_{\mathcal{A}}: \mathcal{Z}^3 \to \{0, 1\}$ be the characteristic function of the array, i.e., $\chi_{\mathcal{A}}(\boldsymbol{s}) = 1$ if a sensor is in position $\boldsymbol{s}$ and $\chi_{\mathcal{A}}(\boldsymbol{s}) = 0$ elsewhere. The number of times the lag $\boldsymbol{d}$ is present in the sparse array defines the autocorrelation function $\Lambda(\boldsymbol{d})$ of $\chi_{\mathcal{A}}: \mathcal{Z}^3 \to \mathcal{N}$. With these definitions, the following result is proved.

Result 1: For a given number of sensors, the numbers of holes and redundancies that must be present in the linear, planar, or volume array satisfy the relation[2]

$$R(3\pi + 2(1 + \alpha_A)) + H(3\pi - 2(1 + \alpha_A)) \geq 2(1 + \alpha_A)M^2 - (M - 1)(3\pi + 2(1 + \alpha_A)) \quad (2.2)$$

where α_A is given in the Appendix.[3]

Proof: Let $\chi_{\overline{\mathcal{D}}}$ be the characteristic function of the coarray associated with the fully populated array of apertures (A_x, A_y, A_z) and $\chi_{\mathbf{0}}: \mathcal{Z}^3 \to \{0, 1\}$ that of lag $\mathbf{0}$ whose Fourier transforms are, respectively, $\frac{\sin \pi(2A_x+1)f_x}{\sin \pi f_x}$ $\frac{\sin \pi(2A_y+1)f_y}{\sin \pi f_y}$ $\frac{\sin \pi(2A_z+1)f_z}{\sin \pi f_z}$ and 1.

As $\Lambda(\boldsymbol{d})$ is the number of times the lag $\boldsymbol{d}$ appears in the array $\mathcal{A}$, the difference

$$\epsilon(\boldsymbol{d}) \stackrel{\text{def}}{=} \Lambda(\boldsymbol{d}) - \chi_{\overline{\mathcal{D}}}(\boldsymbol{d}) - (M - 1)\chi_{\mathbf{0}}(\boldsymbol{d}) \quad (2.3)$$

satisfies for $\boldsymbol{d}$ in $\overline{\mathcal{D}}$: $\epsilon(\boldsymbol{d}) = -1$ if $\boldsymbol{d}$ is a hole, $\epsilon(\boldsymbol{d})$ is equal to the number of redundancies of that lag $\boldsymbol{d}$ if $\boldsymbol{d}$ is in $\mathcal{D}$, except for $\boldsymbol{d} = \mathbf{0}$ in which case $\epsilon(\boldsymbol{d}) = \mathbf{0}$. Consequently, $\sum_{\boldsymbol{d} \in \overline{\mathcal{D}}} |\epsilon(\boldsymbol{d})| = H + R$. As the Fourier transform $E(\boldsymbol{f})$ of the even real function $\epsilon(\boldsymbol{d})$ is real

$$E(\boldsymbol{f}) \leq |E(\boldsymbol{f})| \leq \sum_{\boldsymbol{d} \in \overline{\mathcal{D}}} |\epsilon(\boldsymbol{d})| = H + R.$$

[2]Note that in our formulation, lags $\boldsymbol{d}$ are in $\mathcal{Z}^3$, so our definitions of H and R differ from those of [3, rel. (19)] in the linear case by the multiplicative factor 2.

[3]In particular, it is shown in the Appendix that $\alpha_A \ll 1$ and that $\alpha_A \approx 0.0237$ for apertures ≥ 6.

Therefore, taking the Fourier transform of (2.3) and noting that the Fourier transform $L(\boldsymbol{f})$ of the autocorrelation function $\Lambda(\boldsymbol{d})$ is real nonnegative, the following holds for all $\boldsymbol{f}$:

$$-\frac{\sin\pi(2A_x+1)f_x}{\sin\pi f_x}\,\frac{\sin\pi(2A_y+1)f_y}{\sin\pi f_y}\,\frac{\sin\pi(2A_z+1)f_z}{\sin\pi f_z}-(M-1) \le H+R-L(\boldsymbol{f})\le H+R.$$

After simple manipulations detailed in the Appendix, we obtain

$$\frac{2}{3\pi}(1+\alpha_A)(2A_x+1)(2A_y+1)(2A_z+1)-(M-1)\le H+R. \quad (2.4)$$

Finally, substituting (2.1) in this expression yields (2.2). □

Result 1, identical to [3, rel. (19)] except for the presence of α_A, improves the classic 1-D bound [1], and extends it to 2-D and three-dimensional (3–D) arrays. Surprisingly, this result is invariant with respect to the dimensionality of the array. Putting, respectively, $H = 0$ and $R = 0$ in (2.2) gives lower bounds on R and H, respectively, for redundancy and hole arrays. Whatever the dimensionality of the array may be, we have, for redundancy arrays

$$R \ge \frac{2(1+\alpha_A)M^2}{3\pi+2(1+\alpha_A)}-(M-1)$$

and for hole arrays

$$H \ge \frac{2(1+\alpha_A)M^2}{3\pi-2(1+\alpha_A)}-(M-1)\frac{3\pi+2(1+\alpha_A)}{3\pi-2(1+\alpha_A)}.$$

Thus, for large arrays, the lower bounds provided by [3, rels. (20) and (21)] are approximatively multiplied by 1.0237.

Concerning the bounds on M, Result 1 implies the following.

1) For perfect arrays, i.e., arrays with no redundancy or hole ($R = 0;\ H = 0$), Result 1 implies $2(M^2-M+1)-3\pi(M-1)\le 0$, therefore, $M \in \{2, 3, 4\}$. Thus, from (2.1)

$$M^2-M+1=(2A_x+1)(2A_y+1)(2A_z+1)=3,\ 7,\ \text{or}\ 13.$$

Since the product $(2A_x+1)(2A_y+1)(2A_z+1)$ is prime, the only, nontrivial solutions are

$$M=3 \qquad A_x=3 \qquad A_y=A_z=0$$

and

$$M=4 \qquad A_x=6 \qquad A_y=A_z=0.$$

These are the well-known linear perfect arrays [3] and we prove that the only perfect arrays are linear.

2) For redundancy arrays [3], i.e., arrays with no hole ($H = 0$), Result 1 and (2.1) yield

$$M^2\ge(2A_x+1)(2A_y+1)(2A_z+1)\left(1+\frac{2(1+\alpha_A)}{3\pi}\right) \quad (2.5)$$

which for $A_y = A_z = 0$ gives a tighter lower bound on M than [3, rel. (17)]. However, because of roundoff effect, the improvement provided by (2.5) in the 1-D case is not regular and occurs for only certain values of A. For example, for linear MR (LMR) arrays, $A = 69$ is the lowest value of A for which the lower bound on M provided by [3, rel. (17)] and by (2.5) would be different (respectively, $M \ge 13$ and $M \ge 14$).

3) For hole arrays [3], i.e., arrays with no redundancy ($R = 0$), Result 1 and (2.1) yield

$$(M-1)^2\le(2A_x+1)(2A_y+1)(2A_z+1)\left(1-\frac{2(1+\alpha_A)}{3\pi}\right)-1 \quad (2.6)$$

which for $A_y = A_z = 0$ gives a tighter upper bound on M than [3, rel. (26)]. But, as previously, the improvement in the one-dimensional case is not regular and, for example, for linear MH (LMH) arrays, $A = 51$ is the lowest value of A for which the upper bound on M provided by [3, rel. (26)] and by (2.6) would be different (respectively, $M \le 10$ and $M \le 9$).

III. Design of Sparse Linear and Volume Arrays

To build efficient square and cubic redundancy arrays, two regular structures are known. The first, referred to by Pumphrey [8] as "cross product" (CP) arrays, are constructed from, respectively, two or three identical LMR arrays. A square cross-product array, for example, has a sensor at $\{i, j\}$ if the linear array it is constructed from has a sensor at $\{i\}$ *and* one at $\{j\}$ (see Fig. 2). Note that these structures can be extended to nonidentical LMR arrays. As LMR arrays are built for any M, their optimal aperture A is a function A_M of M. So associated cross-product arrays are defined only for these apertures A_M, for which the number of sensors is M^2 or M^3. As for LMR arrays [5], [4]

$$2.434 \le \lim_{M\to\infty}\frac{M^2}{A_M} \le 3.348$$

therefore, these cross-product structures satisfy, respectively, for the square and cubic arrays with M sensors

$$2.434 \le \lim_{M\to\infty}\frac{M}{A_M} \le 3.348$$

and

$$2.434 \le \lim_{M\to\infty}\frac{M^{2/3}}{A_M} \le 3.348. \quad (3.1)$$

Compared to (2.5), which gives for linear, square, and cubic redundancy arrays $M^2 \ge 2.434A + 1.217$, $M \ge 2.207A + 1.103$, and $M^{2/3} \ge 2.135A + 1.068$, respectively, these cross-product redundancy arrays are potentially efficient. However, we note that the difference between the number of sensors given by the lower bound (2.5) and the one given by (3.1) increases with the dimensionality of the array. A second regular structure was proposed by Greene–Wood (GW) [11] for square arrays. The sensor location (i, j, k) of such an array of aperture A verifies: $i = 0$ or $j = 0$ or $k = 0$ or $i = j = k = 2, \ldots, A$ ($k = 0$ for square array cf. Fig. 2). It gives, respectively, $M = 3A$ and $M = A(3A+4)$ for square and cubic arrays.[4] Compared to (2.5), the GW square array is a potentially efficient redundancy array contrary to the GW cubic array. Naturally, all these structures are not necessarily MR. Table I exhibits, by exhaustive computer search, the number of MR and MH square arrays for apertures up to 6(7 for MH square arrays), two arrays being considered different if none of them can be deduced from the other by an elementary transformation. We find that these arrays are not generally unique. However, GWor cross-product MR arrays exist for each of these apertures (except for $A = 2$).

IV. Conclusion

A general formulation has enabled us to consider the notion of minimum hole and minimum redundancy arrays regardless of the dimensionality of the array. Thanks to this approach, tighter bounds have been given on the numbers of sensors, redundancies, and holes for the linear arrays and similar bounds have been proposed for planar and volume arrays. As an application, the efficiency of regular planar and volume arrays with redundancies but no holes has been deduced (see Fig. 1 for planar arrays). The number of sensors and configurations of square MR and MH arrays obtained by exhaustive computer search has been

[4]Note that a more efficient cubic structure can be obtained by piling up identical GW square arrays for which the number of sensors is $M = 3A(A+1)$.

given. An example of square MR and MH array for each aperture is exhibited up to aperture 7 (see Figs. 2 and 3). Finally, we note that designing simple regular structures of efficient hole arrays, or deducing hole planar and volume arrays from linear hole arrays, still presents a number of obstacles.

APPENDIX
PROOF OF (2.4)

Let $s(\boldsymbol{A}, \boldsymbol{f})$ denote the expression

$$-\frac{\sin \pi(2A_x+1)f_x}{\sin \pi f_x}\,\frac{\sin \pi(2A_y+1)f_y}{\sin \pi f_y}\,\frac{\sin \pi(2A_z+1)f_z}{\sin \pi f_z}.$$

Because explicit calculation of $\max_{\boldsymbol{f}} s(\boldsymbol{A}, \boldsymbol{f})$ is complicated, we shall focus on two slightly smaller values. First, as

$$\max_x \left(-\frac{\sin x}{x}\right) = \frac{2}{3\pi}(1+\alpha')$$

with $\alpha' = 0.0237$ and $\sin x < x$ for $x > 0$, direct manipulations imply

$$\frac{2}{3\pi}(1+\alpha')(2A_x+1)(2A_y+1)(2A_z+1) \le \max_{\boldsymbol{f}} s(\boldsymbol{A}, \boldsymbol{f}).$$

Second, suppose $A_x = \min(A_x, A_y, A_z)$ without loss of generality. For

$$\boldsymbol{f}_0 \stackrel{\text{def}}{=} (f_0, 0, 0) \qquad f_0 \stackrel{\text{def}}{=} \frac{3}{2(2A_x+1)}$$

$$-\frac{\sin \pi(2A_x+1)f_0}{\sin \pi f_0}(2A_y+1)(2A_z+1) = s(\boldsymbol{A}, \boldsymbol{f}_0) \le \max_{\boldsymbol{f}} s(\boldsymbol{A}, \boldsymbol{f}).$$

Using the classical relation between the periodic Fourier transform of a sequence and the Fourier transform of the associated analog waveform

$$\begin{aligned}
&-\frac{\sin \pi(2A_x+1)f_0}{\sin \pi f_0} \\
&\quad = -\sum_{k=-\infty}^{+\infty} \frac{\sin(\pi(2A_x+1)(f_0-k))}{\pi(f_0-k)} \\
&\quad = -\frac{\sin \pi(2A_x+1)f_0}{\pi} \sum_{k=-\infty}^{+\infty} \frac{(-1)^k}{f_0-k} \\
&\quad = -\frac{\sin \pi(2A_x+1)f_0}{\pi}\left(\frac{1}{f_0} + 2f_0 \sum_{k=1}^{+\infty} \frac{(-1)^k}{{f_0}^2-k^2}\right) \\
&\quad = \frac{2}{3\pi}(2A_x+1)\left(1 - \frac{9}{2}\sum_{k=1}^{+\infty} \frac{(-1)^k}{k^2(2A_x+1)^2-\frac{9}{4}}\right) \\
&\quad \stackrel{\text{def}}{=} \frac{2}{3\pi}(2A_x+1)(1+\alpha_A'').
\end{aligned}$$

Therefore,

$$\frac{2}{3\pi}(1+\alpha_A'')(2A_x+1)(2A_y+1)(2A_z+1) \le \max_{\boldsymbol{f}} s(\boldsymbol{A}, \boldsymbol{f}).$$

Combining these two values, (2.4) holds with $\alpha_A \stackrel{\text{def}}{=} \max(\alpha', \alpha_A'')$. We note that α_A'' is decreasing in A_x and a sharp examination of α_A'' shows that $\alpha_A = \alpha_A''$ for $A_x < 6$ (e.g., $\alpha_3 \approx 0.0797$) and $\alpha_A = \alpha' \approx 0.0237$ for $A_x \ge 6$.

REFERENCES

[1] S. De Graff and D. H. Johnson, "Optimal linear arrays for narrow-band beamforming," in *Proc. ICASSP-84*, 1984, pp. 40.8.1–40.8.4.

[2] Y. I. Abramovich, D. A. Gray, A. Y. Gorokhov, and N. K. Spencer, "Comparison of DOA estimation performance for various types of sparse antenna array geometries," in *Proc. EUSIPCO-96*, Trieste, Italy, 1996, pp. 915–918.

[3] D. A. Linebarger, I. H. Sudborough, and I. G. Tollis, "Difference bases and sparse sensor arrays," *IEEE Trans. Inform. Theory*, vol. 39, pp. 716–721, Mar. 1993.

[4] S. U. Pillai, *Array Signal Processing*. New York: Springer Verlag, 1988.

[5] J. Leech, "On the representation of $1, 2, \ldots, n$ by differences," *J. London Math. Soc.*, vol. 31, pp. 160–169, 1956.

[6] E. Vertatschitsch and S. Haykin, "Nonredundant array," *Proc. IEEE*, vol. 74, p. 217, Jan. 1986.

[7] X. Huang, J. P. Reilly, and M. Wong, "Optimal design of linear array of sensors," in *Proc. ICASSP-91*, Toronto, ON, Canada, 1991, pp. 1405–1408.

[8] H. C. Pumphrey, "Design of sparse arrays in one, two, and three dimensions," *J. Acoust. Soc. Amer.*, vol. 93, no. 3, pp. 1620–1628, March 1993.

[9] S. Haykin, J. P. Reilly, V. Kezys, and E. Vertatschitsch, "Some aspects of array signal processing," *Proc. Inst. Elelct. Eng. -F*, vol. 139, no. 1, pp. 1–26, Feb, 1992.

[10] R. A. Haubrich, "Array design," *Bull. Seismol. Soc. Amer.*, vol. 58, pp. 977–991, 1968.

[11] C. R. Greene and R. C. Wood, "Sparse array performance," *J. Acoust. Soc. Amer.*, vol. 63, pp. 1866–1872, 1978.

Bounds on Entropy in a Guessing Game

Alfredo De Santis, Antonio Giorgio Gaggia, and Ugo Vaccaro

***Abstract*—We consider the guessing problem proposed by Massey [1] of a cryptanalyst that wants to break a ciphertext with a brute-force attack. The best strategy he can use is to try out all possible keys, one at time in order of decreasing probability, after narrowing the possibilities by some cryptanalysis. In this correspondence we provide both upper and lower bounds on the entropy of the probability distribution on the secret keys in terms of the number of secret keys and of the average number of trials of the cryptanalyst.**

***Index Terms*—Entropy, guessing, probability.**

I. INTRODUCTION

Massey in [1] considered the problem of a cryptanalyst that, in order to decrypt a ciphertext, must try out all possible secret keys, one at a time, after narrowing the possibilities by some cryptanalysis. Let K be the set of all possible secret keys and let $P = (p_1, \ldots, p_n)$ be the probability distribution where p_i, $i = 1, \ldots, n$, is the probability that the secret key is $k_i \in K$. The strategy that minimizes the number of trials is obviously to guess the possible keys in order of decreasing probability. Without loss of generality, we assume that $p_1 \ge \cdots \ge p_n$. Then the average number of trials of the cryptanalyst is

$$\alpha(P) = \sum_{i=1}^{n} i \cdot p_i.$$

Massey [1] proved that the entropy of P, that is,

$$H(P) = H(p_1, \ldots, p_n) = -\sum_{i=1}^{n} p_i \log p_i$$

Manuscript received July 24, 1996; revised September 7, 1999. This work was supported in part by the Italian Ministry of University and Scientific Research (M.U.R.S.T.) and by the National Council of Research (C.N.R.).

The authors are with Dipartimento di Informatica ed Applicazioni, Università di Salerno, 84081 Baronissi (SA), Italy (e-mail: ads@dia.unisa.it; antgio@dia.unisa.it; uv@dia.unisa.it).

Communicated by C. Crépeau, Associate Editor for Complexity and Cryptography.

Publisher Item Identifier S 0018-9448(01)00466-7.