AFCRL-64-697
AUGUST 1964

Physical and Mathematical Sciences Research Papers
No. 46

Weight Distribution of the Quadratic Residue (71,35) Code

VERA PLESS

DATA SCIENCES LABORATORY PROJECT 5632

AIR FORCE CAMBRIDGE RESEARCH LABORATORIES, OFFICE OF AEROSPACE RESEARCH, UNITED STATES AIR FORCE, L.G. HANSCOM FIELD, MASS.

BLANK PAGE

AFCRL-64-697
AUGUST 1964

Physical and Mathematical Sciences Rese
No. 46

Weight Distribution of the Quadratic Residue (71,35) Code

VERA PLESS

DATA SCIENCES LABORATORY PROJECT 5632

AIR FORCE CAMBRIDGE RESEARCH LABORATORIES, OFFICE OF AEROSPACE RESEARCH, UNITED STATES AIR FORCE, L.G. HANSCOM FIELD, MASS.

Abstract

The hand calculation of the weight distribution of the (71, 35) quadratic residue code is briefly described. This calculation falls into two parts. The first part consists in evaluating the 10×10 determinant given by the power-moment identities, using properties of Van der Monde determinants. The second part of the calculation consists in reducing the six solutions obtained in the first part to one solution. This reduction is accomplished by group theory analysis.

BLANK PAGE

Weight Distribution of the Quadratic Residue (71,35) Code

The code A we are considering is a 35-dimensional code in a vector space V of dimension 71 over the field of two elements. Let V be a vector space of dim p (p a prime, equivalent to -1 mod 8) over the field of two elements. A belongs to the general class of cyclic codes [of dim (p-1)/2] in such a space V, which are left invariant by the coordinate permutations $i \to ai$, as a quadratic residue mod p. (We label the coordinates of a vector from 0 to p-1.) The following facts are known about this class of codes.[1,2] There are two such equivalent codes in the vector space. The code is self-orthogonal, and its orthogonal consists of itself plus the all-one vector. All the weights in the code are divisible by 4, and the minimum weight must satisfy the inequality $(d-1)(d-2) \geq p-1$.[3] By this latter bound the minimum weight in our code must be ≥ 12. A vector of weight 12 is known to exist;[2] hence the minimum weight is 12. If we let A_i be the set of vectors of weight i in the code, we have 13 unknowns: $A_{12}, A_{16}, A_{20}, \ldots, A_{60}$.

If we consider the first power-moment identities[4] that the code must satisfy, we get equations of the following form:

$$\begin{aligned}
A_{12} + \cdots + A_{60} &= c_0 \\
12A_{12} + \cdots + 60A_{60} &= c_1 \\
&\vdots \\
12^{10}A_{12} + \cdots + 60^{10}A_{60} &= c_{10} \qquad (1) \\
12^{11}A_{12} + \cdots + (60^{11}A_{60} - d_{11}A_{60}) &= c_{11} \\
(12^{12}A_{12} - e_{12}A_{12}) + 13^{12}A_{16} + \cdots + 56^{12}A_{56} + (60^{12}A_{60} - d_{12}A_{60}) &= c_{12}
\end{aligned}$$

(Received for publication 5 August 1964)

where the c's, d's, and e's are constants determined by the power-moment identities. The determinant of this set of equations is zero.

It can be proved that $iA_i = (p-i+1)A_{(p-i+1)}$. The use we make of this here is to express A_{12} in terms of A_{60}. Since $12A_{12} = 60A_{60}$, $A_{12} = 5A_{60}$. Using this we express the righthand side of the first eleven equations of (1) in terms of constants and A_{60}. The form of these equations is

$$\begin{aligned} A_{16} + \cdots + A_{56} &= c_0 - g_0 A_{60} \\ 16A_{16} + \cdots + 56A_{56} &= c_1 - g_1 A_{60} \\ &\vdots \\ 16^{10}A_{16} + \cdots + 56^{10}A_{56} &= c_{10} - g_{10} A_{60} \end{aligned} \tag{2}$$

If A_{60} is regarded as a fixed but unknown constant, we form a system of equations whose determinant is Van der Monde and hence nonsingular. Substituting the column of constants into the first column of Eq.(2) and attempting to solve for A_{16} by Cramer's rule, we get a sum of subdeterminants that are 10×10. A determinant of this size usually presents a formidable computation problem, but since these determinants are almost Van der Monde they can be evaluated by hand. The result of this calculation is

$$A_{16} = 71\times 7\times 391 - 56A_{60} \tag{3}$$

We will let G denote the cyclic group of order 35 of quadratic residues mod 71. In this case G is generated by 2. At times an element $\underline{a}$ in G will be considered the coordinate permutation $i \to ai$ of V; at other times $\underline{a}$ will be considered the $\underline{a}$th coordinate index. The context will determine which is meant.

As previously noted, A is invariant under the coordinate permutations in G. Hence the set of vectors of any fixed weight in the code is also invariant under this group. This implies that A_i must be divisible by 35 if neither i nor i-1 is a multiple of 5 or 7. If i or i-1 is divisible by 5 and not 7 (7 and not 5), A_i must be divisible by 7(5). Hence A_{60} is divisible by 7. Since the code is cyclic, each A_i is divisible by 71.

Using these facts and Eq.(3) we will try to determine the possible values for A_{60}. Since the determinant of Eq.(2) is nonsingular, once A_{60} is known we can calculate a unique solution for the remaining weights. By the above, A_{60} is divisible by 71×7, and since $A_{16} \geq 0$, by these divisibility conditions the possible values of A_{60} are the following six numbers: 71×7, 71×14, 71×21, 71×28, 71×35, 71×42.

We are able to limit this set to three solutions by proving that either 35 divides A_{60} or 35 divides $A_{60} - 71\times 7$. This is done by the following argument. If 35 does

not divide A_{60}, there must be a vector v in A of weight 60 which is invariant under the subgroup K (of order 5) of G generated by 2^7. Let E_v be the equivalence class of vectors equivalent to v under the coordinate permutations in G and the cyclic group of order 71; E_v has 71×7 vectors. Our statement holds if we can show that it is impossible to have two equivalence classes of 71×7 vectors in A. Let aK be a coset of K, and -aK be the set of coordinate indices -ak, ak in aK; K and its cosets and minus these sets represent 14 disjoint sets of coordinate indices. Since v must have a zero on its zeroth coordinate and ones on 12 of the above-mentioned 14 sets of coordinate indices, v must have either 25, 30, or 35 ones on the coordinate indices in G. Now it is known[2] that the idempotent of the code has a one on its zeroth coordinate and 35 ones on either G or -G. If v has either 25 or 35 ones on G the addition of the idempotent would yield a vector in A whose weight is not divisible by 4. Thus v has 30 ones on G and 30 ones on -G, or in other words, v has 5 zeros on one coset aK, and 5 zeros on one set -bK; E_v then contains 7 vectors, each with zeros on a different coset of K, in particular a vector w with zeros on K and on one set -cK. If there were another equivalence class in A containing 71×7 vectors of weight 60 it also would contain a vector w' with zeros on K and on one set -dK. The weight of w + w' must then be 10, not divisible by 4. Thus we have three possible solutions for A_{60}: 71×7, 71×35, and 71×42.

The vector v that has ones on K, 2K, 2^2K, 2^3K, 2^4K, 2^5K, -K, -2K, -2^2K, -2^3K, -2^4K, -2^6K is invariant under the group K and is in one of the two quadratic residue codes. This reduces the number of solutions to two: 71×7 and 71×42. The solution A_{60} = 71×42 implies that A_{56} = 71×110; the solution A_{60} = 71×7 implies that A_{56} = 71×670. The case A_{60} = 71×42 was eliminated by determining that more than 71×110 vectors of weight 56 are in the code. This was done by examining the following four vectors of weight 15, which are complements of vectors of weight 56 in the code.

$$w_1 = (0, 36, 38, 43, 44, 45, 46, 47, 54, 58, 63, 64, 66, 67, 70)$$

$$w_2 = (0, 4, 5, 6, 10, 13, 14, 20, 25, 30, 38, 48, 51, 63, 68)$$

$$w_3 = (0, 3, 6, 12, 18, 20, 23, 24, 34, 40, 41, 50, 54, 61, 70)$$

$$w_4 = (0, 5, 20, 22, 30, 36, 38, 39, 43, 44, 46, 47, 61, 64, 67)$$

Each one belongs to a distinct equivalence class under G and the cyclic group of order 71. Each equivalence class was shown to have 35×71 distinct elements; hence there are at least 140 vectors of weight 56 in A. Thus, A_{60} must be 71×7. Using this, the remaining weights are as follows:

$$A_{12} = 35 \times 71 = 2,485$$

$$A_{16} = 2,345 \times 71 = 166,495$$

$$A_{20} = 186,186 \times 71 = 13,219,206$$

$$A_{24} = 4,340,910 \times 71 = 308,204,610$$

$$A_{28} = 37,861,505 \times 71 = 2,688,166,855$$

$$A_{32} = 129,893,225 \times 71 = 9,222,418,975$$

$$A_{36} = 181,404,764 \times 71 = 12,879,738,244$$

$$A_{40} = 103,914,580 \times 71 = 7,377,935,180$$

$$A_{44} = 24,093,685 \times 71 = 1,710,651,635$$

$$A_{48} = 2,170,455 \times 71 = 154,102,305$$

$$A_{52} = 71,610 \times 71 = 5,084,310$$

$$A_{56} = 670 \times 71 = 47,570$$

$$A_{60} = 7 \times 71 = 497$$

Acknowledgments

I wish to thank Eugene Prange for many helpful discussions. One of his results is used in the proof of $iA_i = (p - i + 1)A_{(p-i+1)}$. Mr. Prange also suggested a simple method to show that the above four vectors belong to separate equivalence classes of 35×71 elements.

I also wish to thank Brookhaven National Laboratory, where some of this work was done, for guest privileges.

References

1. A. M. Gleason, private communication.
2. E. Prange, private communication.
3. H. F. Mattson and G. Solomon, A new treatment of Bose-Chaudhuri codes, J. Soc. Indust. Appl. Math. 9:654, December 1961.
4. V. Pless, Power moment identities on weight distributions in error correcting codes, Information and Control 6:147, June 1963.

BLANK PAGE

PHYSICAL SCIENCES RESEARCH PAPERS

No. 1. Central-Force Laws for an Elliptic Orbit, *Kurt Toman, March 1964 (REPRINT).*

No. 2. Structure of 10, 10-Dibromoanthrone, *J. Silverman, N. F. Yannoni, February 1964 (REPRINT).*

No. 3. Ion Dissociation in the Drift Tube of a Time-of-Flight Mass Spectrometer: V. Analytic Solutions of the Flight-Time Shift Equation, *W. W. Hunt, Jr., M. J. Kennedy, February 1964.*

No. 4. Asymptotic Form of the Electron Capture Cross Section in the Impulse Approximation, *R. A. Mapleton, March 1964 (REPRINT).*

No. 5. Intelligibility of Excerpts From Fluent Speech: Effects of Rate of Utterance and Duration of Excerpt, *J. M. Pickett, Irwin Pollack, March 1964 (REPRINT).*

No. 6. Back-Scatter by Dielectric Spheres With and Without Metal Caps, *David Atlas, Kenneth M. Glover, March 1964 (REPRINT).*

No. 7. An Adaptive Filter for the Design of Ionospheric Disturbance Detectors (U), *Richard D. Smallwood, 1/Lt, USAF, February 1964 (SECRET).*

No. 8. The Nonlinear Interaction of an Electromagnetic Wave With a Time-Dependent Plasma Medium, *Robert J. Papa, April 1964.*

No. 9. Drastic Reduction of Warm-up Rate Within a Dewar System by Helium Desorption, *Peter D. Gianino, January 1964.*

No. 10. The Antipodal Image of an Electromagnetic Source, *Kurt Toman, April 1964 (REPRINT).*

No. 11. Radiation Forces in Inhomogeneous Media, *E.J. Post, April 1964 (REPRINT).*

No. 12. Progressive Failure Prediction, *Walton B. Bishop, April 1964 (REPRINT).*

No. 13. Visual Data Transmission, *Ronald J. Massa, 1/Lt, USAF, April 1964.*

No. 14. Rydberg Absorption Series of N_2, *M. Ogawa and Y. Tanaka, May 1964 (REPRINT).*

No. 15. 600-A Band of Helium, *Y. Tanaka and K. Yoshino, May 1964 (REPRINT).*

No. 16. Charge Transfer Studies With a Time-of-Flight Mass Spectrometer: II. Kinetic Analysis, Including Attenuation of Both Neutrals and Ions by Scattering, *W. W. Hunt, Jr., May 1964.*

No. 17. Photo-Induced Electron Transfer in Dye-Sulphydryl Protein Complex, *Eiji Fujimori, May 1964, (REPRINT).*

No. 18. Intelligibility of Excerpts From Fluent Speech: Auditory vs. Structural Context, *Irwin Pollack and J.M. Pickett, May 1964, (REPRINT).*

No. 19. A Study of Transverse Modes of Ruby Lasers Using Beat Frequency Detection and Fast Photography, *C. Martin Stickley, May 1964.*

No. 20. Some Effects of Semantic and Grammatical Context on the Production and Perception of Speech, *Philip Lieberman, June 1964 (REPRINT).*

No. 21. Infrared Absorption of Magnesium Stannide, *Herbert G. Lipson and Alfred Kahan, June 1964 (REPRINT).*

No. 22. On the Optimum Design of Multipath Signals, *Neil J. Bershad, 1/Lt USAF, June 1964.*

No. 23. Area Properties of Television Pictures, *S. Nishikawa, R.J. Massa, J.C. Mott-Smith, June 1964.*

No. 24. A Geometric Study of Coherence Properties of Partially Polarized Electromagnetic Radiation, *E.F. Bolinder, June 1964.*

No. 25. The Preparation of High-Purity Boron via the Iodide, *A.F. Armington, G.F. Dillon, and R.F. Mitchell, June 1964 (REPRINT).*

No. 26. An Interpretation of the Far-Field Effects of a Rocket in the Ionosphere (U), *Thomas D. Conley and James E. Higgins, June 1964 (SECRET).*

No. 27. A Radon-Nikodym Theorem in Dimension Lattices, *S.S. Holland, Jr., June 1964 (REPRINT).*

No. 28. Plasma Produced Antenna Pattern Distortion, *Daniel J. Jacavanco, June 1964.*

No. 29. Geometry and First-Order Error Statistics for Three- and Four-Station Hyperbolic Fixes on a Spherical Earth, *Edward A. Lewis, June 1964.*

No. 30. Ion Dissociation in the Drift Tube of a Time-of-Flight Mass Spectrometer: III Flight-Time Shift Equations for Spurious Fragment Peaks Arising From Charge Transfer and Dissociation Reactions Occurring Inside the Potential Barrier, *W.W. Hunt, Jr., June 1964.*

No. 31. Dolph-Tchebyscheff Arrays of Many Elements and Arbitrary Uniform Spacing, *Charles J. Drane, Jr., June 1964.*

PHYSICAL SCIENCES RESEARCH PAPERS (Continued)

No. 32. Measurement of Noise Figure of an X-Band Waveguide Mixer with Tunnel Diode, *Gustav H. Blaeser, July 1964.*

No. 33. Transient Reflection and Transmission of a Plane Wave Normally Incident Upon a Semi-Infinite Anisotropic Plasma, *Carl T. Case, 1/Lt, USAF, July 1964.*

No. 34. Low-Temperature Far-Infrared Spectra of Germanium and Silicon, *Peter J. Gielisse, James R. Aronson and Hugh G. McLinden, June 1964.*

No. 35. Absorption Coefficients of Carbon Monoxide in the 1006-600-A Wavelength Region, *R.E. Huffman, J.C. Larrabee and Y. Tanaka, July 1964 (REPRINT).*

No. 36. Asymptotic Form of the Electron Capture Cross Section in First Born and Distorted Wave Approximations, *R.A. Mapleton, July 1964 (REPRINT).*

No. 37. A Computer Approach to Laser Design, *T.G. Purnhagen and J. Lubelfeld, July 1964 (REPRINT).*

No. 38. Apparent Sky Temperatures at Millimeter-Wave Frequencies, *Karl N. Wulfsberg, July 1964.*

No. 39. Observation of 2,1 Charge Transfer in a TOF Mass Spectrometer (Text of a paper presented at the Southwestern Meeting of the American Physical Society at Tucson, Arizona, on 28 February 1964), *W.W. Hunt, Jr., and K.E. McGee, July 1964.*

No. 40. PMR Bi-Static Results During the Period 13 August to 14 December 1962, *T.D. Conley, July 1964 (SECRET).*

No. 41. EM Pulses From 1962 USSR Nuclear Tests, Extracted From Sferics Records (U), *A. Ganio and J.L. Heckscher, Capt, USAF, July 1964 (SECRET-RD).*

No. 42. Dislocation Structures in Single-Crystal Al_2O_3, *D.L. Stephens and W.J. Alford, August 1964 (REPRINT).*

No. 43. Anomalies in VLF Signals Observed During High-Altitude Nuclear Tests, 1962, *Alma Ganio, August 1964 (SECRET-RD).*

No. 44. Molecular Structure of 2-(4'-amino-5'-azamethenyl pyrimidyl)-3 pentene-4-ol, *N.F. Yannoni and Jerry Silverman, August 1964 (REPRINT).*

No. 45. Output Power from GaAs Lasers at Room Temperature, *C.C. Gallagher, P.C. Tandy, B.S. Goldstein and J.D. Welch, August 1964 (REPRINT).*

No. 46. Weight Distribution of the Quadratic Residue (71,35) Code, *Vera Pless, August 1964.*

BLANK PAGE