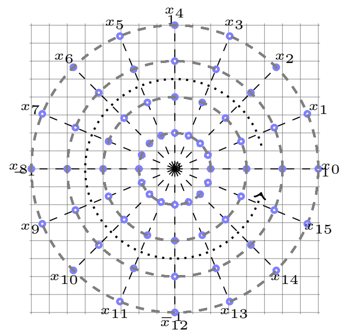
Geometrical Representation for Number-theoretic Transforms

H. M. de Oliveira and R. J. Cintra

***Abstract*— This short note introduces a geometric representation for binary (or ternary) sequences. The proposed representation is linked to multivariate data plotting according to the radar chart. As an illustrative example, the binary Hamming transform recently proposed is geometrically interpreted. It is shown that codewords of standard Hamming code $\mathcal{H}(N=7,k=4,d=3)$ are invariant vectors under the Hamming transform. These invariant are eigenvectors of the binary Hamming transform. The images are always inscribed in a regular polygon of unity side, resembling triangular rose petals and/or "thorns". A geometric representation of the ternary Golay transform, based on the extended Golay $\mathcal{G}(N=12,k=6,d=6)$ code over $\mathrm{GF}(3)$ is also showed. This approach is offered as an alternative representation of finite-length sequences over finite prime fields.**

***Keywords*— Finite fields, Hamming binary transforms, Golay ternary transforms, geometric representations.**



(a)

Fig. 1. Constellation for $N=16$ and $p=5$. Each radial axis corresponds to a message symbol. The arrow indicates the symbol ordering.

I. Introduction

Discrete transforms defined over a finite field are signal processing tools capable of providing Fourier analysis [1], [2], [3] while operating in error-free structure. Because its arithmetic is performed in a finite field, fixed-point implementations can provide exact computation and simple hardware requirements. Several signal processing contexts were benefited by finite fields transforms [4], [5], [6], [7], [8] with applications linked to the computation of the discrete convolution by means of modular arithmetic and to image processing methods [9], [10]. Number-theoretic transforms (NTTs) are finite-field transforms that operate over $\mathrm{GF}(p)$, where p is a prime number, as opposed to operating over the extension field $\mathrm{GF}(q)$, where q is a power of a prime. Such particular results in simple, error-free architectures while preserving an analogy to real-valued computation.

Besides their applications in signal processing, NTTs have been linked to error correcting codes. Based on the Fourier NTT and the Hartley NTT, the Fourier and Hartley codes were introduced [11], [12]. Conversely, popular error-correcting codes [13], such as the Hamming [14] and Golay codes [15], inspired the introduction of the Hamming number-theoretic transform (HamNTT) [16] and the Golay number-theoretic transform (GNTT) [16] which extend the theory introduced in [17], [18]. In fact, an isomorphism between linear codes and transforms was identified in [16].

The goal of this paper is to introduce a representation for sequences over $\mathrm{GF}(p)$ as a tool for the investigation of number-theoretic transforms.

H. M. de Oliveira, Departamento de Estatística, Universidade Federal de Pernambuco, Recife, PE, e-mail: hmo@de.ufpe.br; R. J Cintra, Departamento de Estatística, Universidade Federal de Pernambuco, Recife, PE, e-mail: rjdsc@de.ufpe.br.

II. Geometric representation

Let $\mathrm{GF}(p)$ be a Galois field of order p, where p is a prime number. A message of length N is a sequence $\mathbf{x} = [x_0, x_1, \ldots, x_{N-1}]$ such that $x_i \in \mathrm{GF}(p)$, $i = 0, 1, \ldots, N-1$. Based on the radar representation [19] (also referred to as web chart or spider chart), we propose a geometrical representation for such messages. The geometric representation consists of mapping the message symbols in points on the complex plane according to the following expression:

$$z_k = x_k \pmod p \cdot \exp\left(j\frac{2\pi}{N}k\right), \quad k = 0, 1, \ldots, N-1. \tag{1}$$

The set of points $\{z_0, z_1, \ldots, z_{N-1}\}$ defines a constellation on which a geometric shape composed of polygons and segments can be derived.

The geometric representation is constructed according to the following procedure:

1) Locate on the complex plane the loci of the Nth roots of the unity $e^{j\frac{2\pi}{N}k}$, $k = 0, 1, \ldots, N-1$;
2) Scale each root of the unity by the corresponding symbol x_k as shown in (1) and plot the resulting point z_k on the plane;
3) Draw line segments joining the points z_{k+1} and z_k to obtain the geometric representation.

For instance, Figure 1 shows the required constellation for 16-point messages over $\mathrm{GF}(5)$.

III. Geometrical Representation of Binary Sequences

The special case $p=2$ and $N=7$ is suitably linked to the Hamming NTT [16]. Based on the binary Hamming code

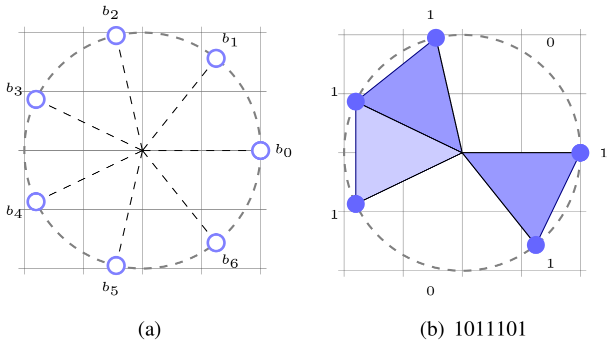


Fig. 2. Geometric representation of codewords. (a) Geometric space. Circles are filled or not according to the bits of the word. (b) Representation of the word [1011101].

$\mathcal{H}(7,4,3)$, we get the 7×7 binary Hamming NTT, whose transformation matrix is [18]

$$\mathbf{T}_{\text{HamNTT}} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

This transform has the property that its eigenvector matrix is equal to the generator matrix of the code $\mathcal{H}(7,4,3)$, i.e.:

$$\text{eig}\left\{\mathbf{T}_{\text{HamNTT}}\right\} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} = \mathbf{G}.$$

Input data is represented by $\mathbf{x} = [b_0, b_1, \ldots, b_6]$, where $b_k \in \{0,1\}$, $k = 0,1,\ldots,6$. Such sequence is used to create small circles on the dashed circumference shown in Figure 2(a). If $b_k = 1$, then a small circle filled in color is placed at position $z_k = e^{j\frac{2\pi}{7}k}$; otherwise, if $b_k = 0$, then the small circles are not generated. The next step is the petal creation: any two consecutive filled circles forms a triangle with the origin $(0,0)$ producing a petal (alternately shaded in light and dark color). Points b_0 and b_6 (cyclical geometry) are understood as neighbors. Figure 2(b) represents the byte [1011101]. The above linear transform maps 7-bit sequences over 128 possible patterns. In the Appendix, Figure 7 lists all 7-bit sequences in the proposed representation. Figure 4(a)-(b) shows a particular sequence and its associate transformed sequence according to the HammNTT. Some sequences are invariant to the Hamming NTT such as $\mathbf{x} = [1100001]^\top$ which satisfies $\mathbf{T}_{\text{HamNTT}} \cdot \mathbf{x} = \mathbf{x}$. Figure 4(c)-(d) displays an invariant sequence and its transformed sequence.

IV. Geometrical Representation of the Ternary Golay Transform

For the ternary Golay codes, the extended Golay code has parameters $\mathcal{G}(N = 12, k = 6, d = 6)$ over $GF(3)$. The new geometric space can be constructed by taking now a new

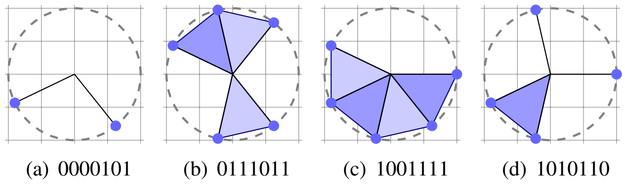


Fig. 3. Geometric representation (a) only thorns, (b)-(c) petals, and (d) thorns and petals.

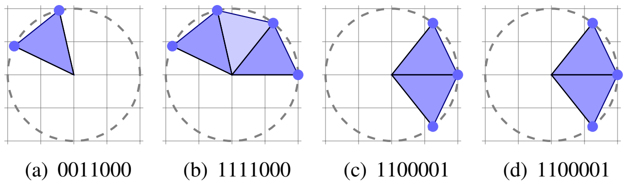


Fig. 4. (a)-(b) A sequence and its associate Hamming NTT sequence. (c)-(d) An invariant sequence to the Hamming NTT.

ensemble of "representative complex points" according to:

$$q_k = r_i \cdot \exp\left(j\frac{2\pi}{12}k\right), \quad i = 0,1,2;\ k = 0,1,\ldots 11, \quad (2)$$

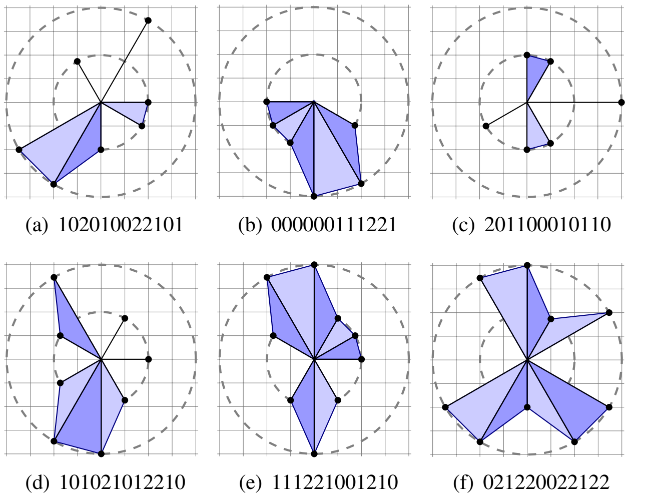
where $r_i = i$. Noticing that $2 \equiv -1 \mod 3$, we can write the associate Golay NTT matrix as follows:

$$\mathbf{T}_{\text{EG}}^{(1)} = \begin{bmatrix} 1 & -1 & -1 & -1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & -1 & 1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & -1 & 1 & -1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ -1 & 1 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & 1 & 1 & -1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ -1 & -1 & 1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & -1 & 1 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & -1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 1 & -1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 1 & -1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ -1 & 1 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & -1 & -1 & 0 & -1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

The above matrix can be efficiently implemented in hardware since it does not require any multiplication operations as its entries are over $\{0, \pm 1\}$. Thus the Golay NTT requires only additions in order to be computed and it is applicable to any sequence of the $\{\text{GF}(3)\}^{12}$-space.

Illustrative examples of the effect of the Golay number-theoretic transform [16] on ternary vectors of length 12 are shown in Figures 5 and 6. Note that complex symbols are always vertices of one of the two dodecagons. Again, colors light blue and dark blue are adopted alternatively in consecutive petals, without major implications, except in improving the visualization. Three codewords were chosen at random: [102010022101], [000000111221], and [201100010110]. By applying the Golay NTT to these sequences, we obtain the following transformed sequences:

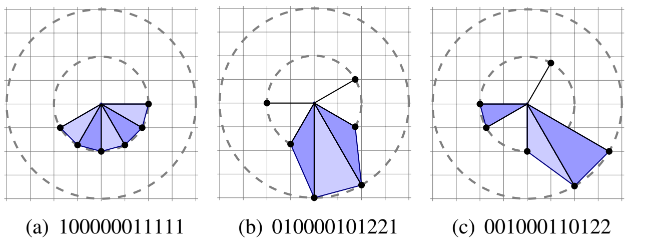
$$\mathbf{T}_{\text{EG}}^{(1)} \cdot [102010022101]^\top = [101021012210],$$
$$\mathbf{T}_{\text{EG}}^{(1)} \cdot [000000111221]^\top = [111221001210]^\top,$$
$$\mathbf{T}_{\text{EG}}^{(1)} \cdot [201100010110]^\top = [021220022122].$$



(a) 102010022101 (b) 000000111221 (c) 201100010110

(d) 101021012210 (e) 111221001210 (f) 021220022122

Fig. 5. Golay NTT pairs. Input data: (a), (b), and (c); transformed data: (d), (e), and (f), respectively.



(a) 100000011111 (b) 010000101221 (c) 001000110122

Fig. 6. Golay NTT pairs: Invariant sequences.

Invariants of the Golay NTT can the readily obtained from the generator matrix. For instance, the following codewords are invariants: [100000011111], [010000101221], and [001000110122], as demonstrated by:

$$\mathbf{T}_{\text{EG}}^{(1)} \cdot [100000011111]^\top = [100000011111],$$
$$\mathbf{T}_{\text{EG}}^{(1)} \cdot [010000101221]^\top = [010000101221],$$
$$\mathbf{T}_{\text{EG}}^{(1)} \cdot [001000110122]^\top = [001000110122].$$

In the Appendix, Figure 8 shows a subset of the possible words.
the Hamming or Golay codes, which are *self-dual* codes [20]. Such codes could be employed to obtain new number-theoretic

V. Conclusions

This note introduces a geometric representation for finite sequences of elements defined over a finite field. This approach provides a defiant reading for the Hamming and Golay transforms. To the best of our knowledge, no similar proposal to convert sequences into images was found, which consists of assigning angles to the position of the symbol in the sequence as described in (1). Phases (angles) are meaningless, as in radar charts. Such a representation has potential applications in several fields of error correcting codes and signal processing over finite fields, including: (i) RLE run length encoding, (ii) burst error correcting codes, (iii) binary SP, and (iv) theory of filter banks. The proposed approach can lead to new insights and interpretations in the design of coding and signal processing methods dedicated to sequences over finite fields. As future research, we aim at deriving extended versions of transforms. As shown in the Appendix, several geometric and symmetry patterns arise that can be further investigated. Such symmetries might lead to a better understanding of practical issues in programming and in hardware implementation linked to the discussed codes.

Acknowledgements

The second author acknowledges the support from CNPq.

References

[1] J. M. Pollard, "The fast Fourier transform in a finite field," *Math. Comput.*, vol. 25, pp. 365–374, Apr. 1971.

[2] D. Harvey, "Faster arithmetic for number-theoretic transforms," *Journal of Symbolic Computation*, vol. 60, pp. 113–119, 2014.

[3] A. C. Mert, E. Karabulut, E. Ozturk, E. Savas, and A. Aysu, "An extensive study of flexible design methods for the number theoretic transform," *IEEE Transactions on Computers*, 2020.

[4] T. Cooklev, A. Nishihara, and M. Sablatash, "Theory of filter banks over finite fields," in *Proceedings of APCCAS'94-1994 Asia Pacific Conference on Circuits and Systems*, 1994.

[5] G. Jullien, R. Krishnan, and W. Miller, "Complex digital signal processing over finite rings," *IEEE Transactions on Circuits and Systems*, vol. 34, pp. 365–377, Apr. 1987.

[6] S. Hegde and R. Nagapadma, "Medical image compression scheme using number theoretic transform," in *Computer Vision and Machine Intelligence in Medical Image Analysis*, pp. 43–53, Springer, 2020.

[7] T. Toivonen and J. Heikkila, "Video filtering with fermat number theoretic transforms using residue number system," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 1, pp. 92–101, 2005.

[8] E. Ozcan and A. Aysu, "High-level-synthesis of number-theoretic transform: A case study for future cryptosystems," *IEEE Embedded Systems Letters*, 2019.

[9] S. Boussakta and A. G. J. Holt, "Number theoretic transforms and their applications in image processing," *Advances in imaging and electron physics*, vol. 111, pp. 1–90, 1999.

[10] I. Gertner, "Image scanning according to lines on finite fields," in *Applications of Digital Image Processing XII* (A. G. Tescher, ed.), vol. 1153, pp. 285–293, International Society for Optics and Photonics, SPIE, 1990.

[11] R. M. Campello de Souza, R. M. Cardim Britto, and H. M. de Oliveira, "Códigos de Hartley em corpos finitos," in *Anais do XXIX Simpósio Brasileiro de Telecomunicações – SBrT'1*, (Curitiba, PR), 2011.

[12] H. M. de Oliveira, C. M. F. Barros, and R. M. Campello de Souza, "Fourier codes and Hartley codes," in *Anais do XXV Simpósio Brasileiro de Telecomunicações (SBrT'07)*, (Recife, PE), Sept. 2007.

[13] S. Lin and D. J. Costelo, *Error Control Coding*. Englewood Cliffs: Prentice Hall, 2004.

[14] R. W. Hamming, "Error detecting and error correcting codes," *Bell Labs Technical Journal*, vol. 29, 1950.

[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North Holland, 1977.

[16] A. J. A. Paschoal, R. M. Campello de Souza, and H. M. de Oliveira, "The Hamming and Golay number-theoretic transforms," in *Anais do XXV Simpósio Brasileiro de Telecomunicações (SBrT'18)*, (Campina Grande, PB), 2018.

[17] R. M. Campello de Souza, E. S. V. Freire, and H. M. de Oliveira, "Fourier codes," in *Proceedings of the 10th International Symposium on Communication Theory and Applications*, (Ambleside, UK), 2009.

[18] A. J. A. Paschoal, H. M. de Oliveira, and R. M. Campello de Souza, "Novas relações na matriz de transformação da transformada numérica de Pascal," in *Proceeding Series of the Brazilian Society of Applied and Computational Mathematics*, vol. 6, 2018.

[19] Y. Albo, J. Lanir, P. Bak, and S. Rafaeli, "Off the radar: Comparative evaluation of radial visualization solutions for composite indicators," *IEEE Transactions on Visualization and Computer Graphics*, vol. 22, no. 1, pp. 569–578, 2016.

[20] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*. Springer Science & Business Media, 2013.

Appendix

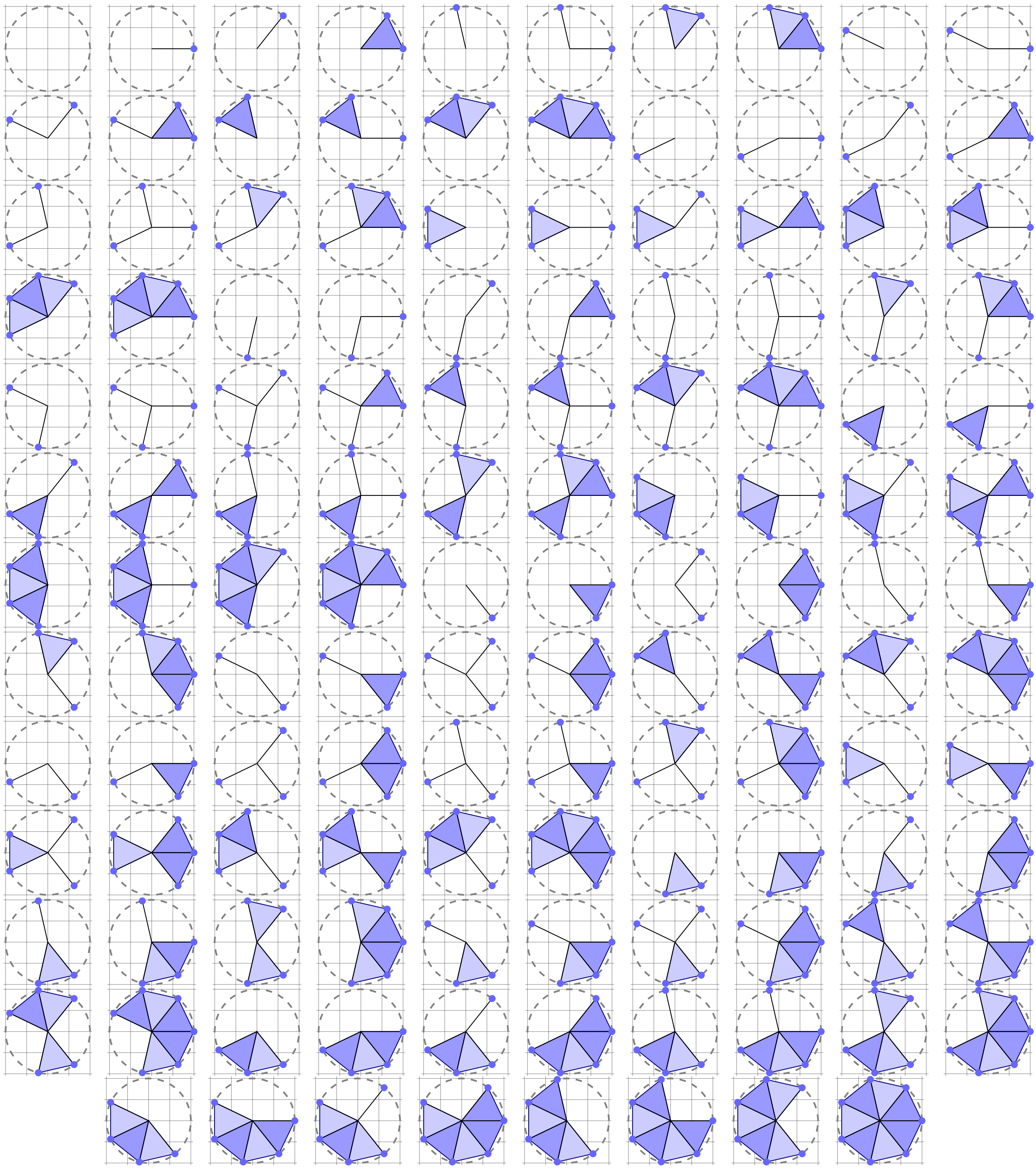


Fig. 7. Geometric representation of all binary 7-tuple.

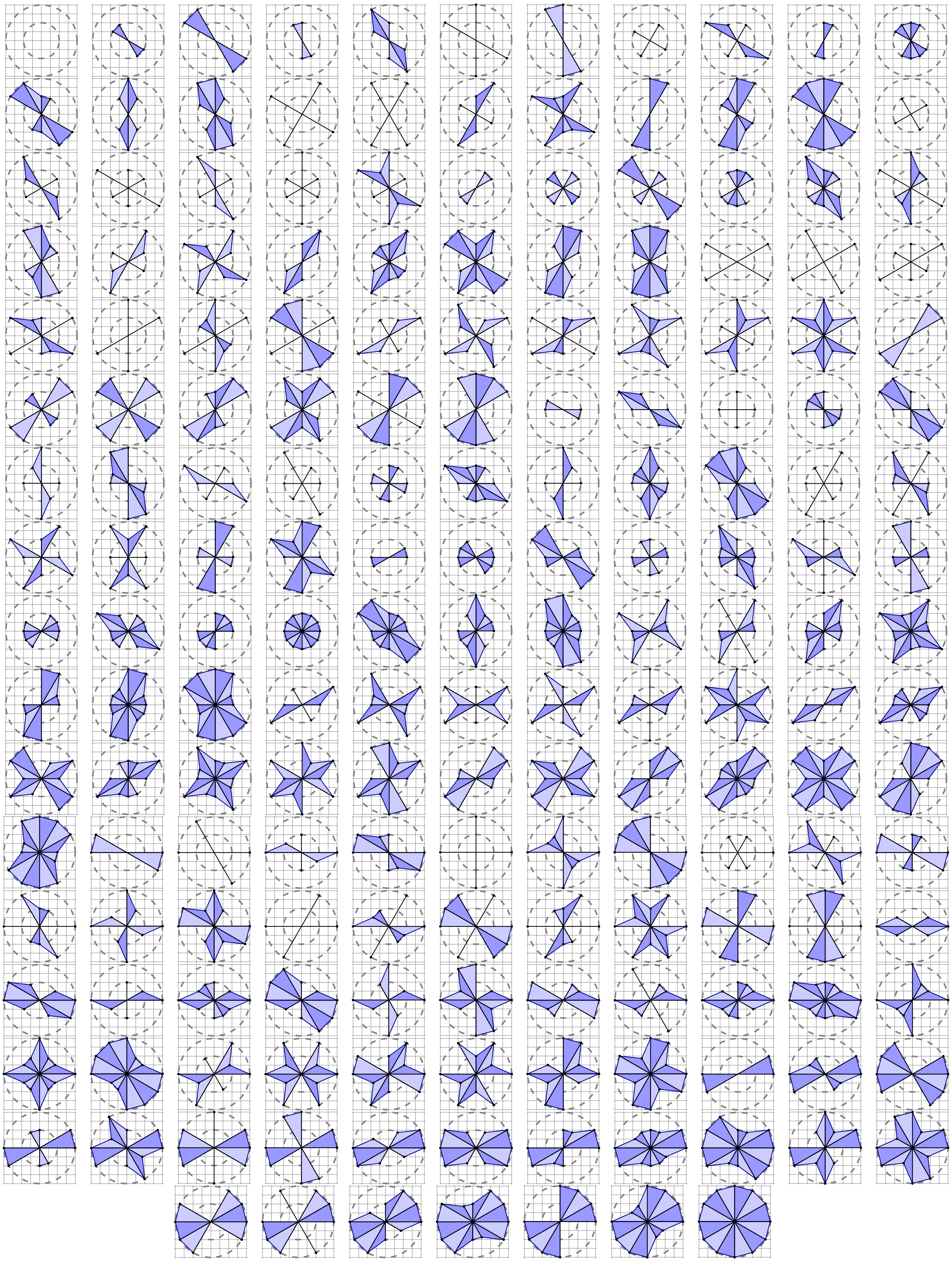


Fig. 8. Geometric representation of selected words of the discussed ternary Golay transform.