Rendiconti di Matematica, Serie VII Volume 30, Roma (2010), 67-76

Some recent results in finite geometry and coding theory arising from the Gale transform

ANTONIO COSSIDENTE – ANGELO SONNINO

Dedicated to Professor Marialuisa de Resmini

ABSTRACT: The Gale transform is an involution on sets of points in a projective space. It plays a crucial role in several different subjects, such as algebraic geometry, optimization, coding theory, and so on. We give a brief survey—from a finite geometry point of view—on the algebraic and geometrical implications of the Gale transform with emphasis on its applications to coding theory, and describe some recent results.

1 – Introduction

The Gale transform of a set \mathcal{T} consisting of γ labelled points of a projective space PG(r,q) is an involution which maps \mathcal{T} into a set \mathcal{T}' consisting of γ labelled points of PG(s,q), defined up to automorphisms of PG(s,q), with $\gamma = r + s + 2$.

The simplest way to define the Gale transform of a set of points is in terms of projective coordinates. Choose homogeneous coordinates in such a way that the coordinates of the points of \mathcal{T} are the rows of the matrix

$$\begin{pmatrix} I_{r+1} \\ A \end{pmatrix},$$

where I_n denotes the $n \times n$ identity matrix and A is an $(s+1) \times (r+1)$ matrix. Then, the Gale transform of \mathcal{T} is the set \mathcal{T}' consisting of the points of PG(s,q)

KEY WORDS AND PHRASES: Gale transform – Linear code – Mathieu group – Cap A.M.S. CLASSIFICATION: 51E20, 94B27.

whose homogeneous coordinates are the rows of the matrix

$$\binom{\tau_A}{I_{s+1}},$$

where \mathcal{A} is the transpose matrix of A.

Although from the definition itself one may doubt whether the Gale transform has any geometry at all in the classical projective sense, the research work carried out over more than two centuries by some of the most important mathematicians is there to show that it is not true.

The first historical occurrency of a result related to the Gale transform is the following theorem which appeared in Pascal's "Essay Pour Les Coniques", see [24].

THEOREM 1.1. (Pascal, 1640) The vertices of two triangles which are circumscribed around the same conic lie on another conic.

Basically, the six points involved in Theorem 1.1 consitute a set of points which is the Gale transform of itself. At an early stage, finding sets of points which are the Gale transform of themselves represented the main goal of mathematicians dealing with the Gale transform. After Pascal, sets that are the Gale transform of themselves appeared in the work of Hesse [17, 18], von Staudt [26], Weddle [27], Zeuthen [29], Dobriner [11], Sturm [25], Rosanes [22, 23], Castelnuovo (who called two sets of points that are the Gale transform of one another "gruppi associati di punti") [3], and many others.

However, it was Coble—whose work had remarkable applications to theta functions and Jacobians of curves, see [4, 5, 6, 7]—the first who studied the Gale transform in a more general setting, starting off with the following alternative definition formulated in terms of matrices over a field.

Let \mathbb{K} be a field and r, s two integers not less than 1. Set $\gamma = r + s + 2$. Consider a subset Γ of a projective spaces of dimension r and a subset Γ' of a projective space of dimension s. Further, let Γ and Γ' be represented by a $\gamma \times (r+1)$ matrix G and a $\gamma \times (s+1)$ matrix G' respectively. Then Γ' is said to be the Gale transform of Γ if there is a nonsingular diagonal $\gamma \times \gamma$ matrix Dsuch that ${}^{T}GDG = 0$.

Whitney [28] and Gale [14] developed similar ideas in the affine case. Later on, Goppa—see [15] and [16] for instance—studied the Gale transform from a coding theory point of view. It is well known that in coding theory the Gale transform is the passage from a code to its dual; Goppa proved that a code defined by the set of GF(q)-rational points on a certain algebraic curve is dual to another code of similar nature.

What we have seen so far is just a quick outline of the rich history of the Gale transform, which has implications in many other branches of modern mathematics such as optimization, group theory, linear spaces, scheme theory, and so on. A full historical treatise on the development of the Gale transform over more than 150 years is well beyond the scope of these notes. For a more detailed historical account on the Gale transform the interested reader is referred to [12] and the references therein.

2 – Preliminary results

The first crucial result concerning the Gale transform of sets of points in finite projective spaces is stated in the following theorem.

THEOREM 2.1. The Gale transform of the projective line PG(1,q), with $q \ge 4$, is a normal rational curve of PG(q-2,q).

The result of Theorem 2.1 was already known to Goppa, as it is related with the so-called Goppa duality among the error correcting codes bearing his name [15, 16]. In [8] there is an alternative proof of this result which is based only on the properties of finite fields.

A natural generalisation of Theorem 2.1 in the finite case, if q is large enough, is the following result.

COROLLARY 2.2. If ℓ is a line in some projective space PG(r, q) and $\mathcal{T} \subseteq \ell$, with $|\mathcal{T}| = r + s + 2$, then the Gale transform \mathcal{T}' of \mathcal{T} is contained in the unique normal rational curve of PG(s, q) containing the fundamental frame.

The proof of Corollary 2.2 is based on the fact that the Gale transform of any subset of points on a line in a projective space PG(r,q) of higher dimension is independent of the embedding of the line in the space. This can be clarified by means of a simple example obtained with the aid of MAGMA [2].

In the projective plane PG(2, 4), where (X_1, X_2, X_3) are projective homogeneous coordinates, consider without loss of generality the line $\ell : X_3 = 0$ whose point set is $\{(1,0,0), (0,1,0), (1,\omega,0), (1,\omega^2,0), (1,1,0)\}$, with ω a primitive element of GF(4). With respect to the Gale transform, the essential part of ℓ is the subset $\{1, \omega, 0\}, (1, \omega^2, 0), (1, 1, 0)\}$ which—after truncation at the second coordinate—gives rise to the points (1, 1, 1) and $(1, \omega, \omega^2)$. By adding the fundamental points of PG(2, 4) we get a conic of PG(2, 4).

Similarly, for q = 5 it can be observed that a line of PG(2, 5) is mapped by the Gale transform onto a twisted cubic of PG(3, 5).

The following result is an important consequence of [19, Theorem 27.5.4].

PROPOSITION 2.3. The Gale transform of a k-cap in a projective space $PG(r,q), k \ge r+4$, is a k-cap in PG(k-r-2,q).

What we have seen so far can be summarized in the following fundamental result, see [8].

THEOREM 2.4. Let \mathcal{T} be any set consisting of k of points in $PG(r,q), r \geq 2$ and $k \geq r+4$. Then the Gale transform \mathcal{T}' of \mathcal{T} is a k-cap in PG(k-r-2,q).

Sometimes it is convenient to have some control over the automorphism groups associated to the geometrical objects obtained in some peculiar way. With this respect, the Gale transform has an interesting behaviour, as it is shown by the following result [8].

PROPOSITION 2.5. Let \mathcal{K} be a k-cap in PG(r, q) and \mathcal{K}' its Gale transform. Then \mathcal{K} and \mathcal{K}' have isomorphic collineation groups.

3- Self-associated sets

A set of points which is the Gale transform of itself is called a self-associated set. Actually, at an early stage the study of the Gale transform was mainly devoted to finding self-associated sets of points with some prescribed properties, see [12] for details and historical information. Some more recent results concerning self-associated sets from an algebraic geometry point of view can be found in [13].

Unlike the classical case, in finite geometry self-associated sets are somehow rare, due to the great number of constrains that the condition of being selfassociate imposes over sets of points in a finite projective space. What follows provides a typical example of such results.

- A conic C in PG(2, q) is self-associated if and only if q = 5. In fact, $\gamma = |C| = q + 1$ and from $\gamma = r + s + 2$, r = s = 2 it follows q = 5.
- In PG(r,q) no self-associated set is the complement of a hyperplane if q is odd. Indeed, if π is a hyperplane of PG(r,q), then $\gamma = q^r = 2(r+1)$, and this equality cannot hold unless q is even.
- The complement of a plane in PG(3, q) is self-associated if and only if q = 2. Indeed, if π is a plane in PG(3, q), then $\gamma = |PG(3, q) \setminus \pi| = q^3$ implies $q^3 = 8$, and hence q = 2.
- The complement of a hyperplane in PG(r, 2) is a self-associated set if and only if r = 3. Indeed, let π be a hyperplane of PG(r, 2). Then, $\gamma = |PG(r, 2) \setminus \pi| = 2^r$. If r = s then $2^{r-1} = r + 1$, which implies r = 3.

What we have just seen can be summarised as follows, see [8].

LEMMA 3.1. The only finite projective space containing a self-associated set which is the complement of a hyperplane is PG(3,2).

4- The Gale transform of an elliptic quadric in $\mathrm{PG}(3,3)$ and the Mathieu groups

In this section we show an interesting connection among the group of an elliptic quadric of PG(3,3) and the Mathieu groups M_{11} , M_{12} obtained by means of the Gale transform.

Let \mathcal{E} be the elliptic quadric of PG(3,3) whose points are

$$\begin{split} P_1 &= (1,0,0,0), \quad P_2 &= (0,1,0,0), \quad P_3 &= (0,0,1,0), \\ P_4 &= (0,0,0,1), \quad P_5 &= (1,1,1,0), \quad P_6 &= (1,0,2,1), \\ P_7 &= (1,2,1,2), \quad P_8 &= (1,1,2,2), \quad P_9 &= (1,2,0,1), \\ P_{10} &= (0,1,1,1). \end{split}$$

Their coordinate vectors are the rows of the matrix

$$\begin{pmatrix} I_4 \\ A \end{pmatrix}.$$

The matrix associated to the Gale transform \mathcal{E}' of \mathcal{E} is

$$\begin{pmatrix} {}^{\tau}\!A \\ I_6 \end{pmatrix},$$

where

$${}^{T}\!A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 2 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 & 1 \end{pmatrix}.$$

The rows of ${}^{\tau}\!A$ generate a vector space $V_1 = V(4,3)$.

Let V = V(10,3) be a 10-dimensional vector space over \mathbb{F}_3 equipped with the standard scalar product. Then, the orthogonal complement of V_1 in V is $V_1^{\perp} = V(6,3) = V_2$.

The 10-caps in PG(5,3) whose points can be arranged to produce the rows of a 10×6 matrix whose columns span a vector space like the above V_2 are called dual 10-caps of \mathcal{E} .

Consider the (unique up to isomorphisms) Steiner System S = S(3, 4, 10)

whose points are the points of \mathcal{E}' and blocks are as follows:

$\{P_4, P_5, P_7, P_9\},\$	$\{P_1, P_2, P_3, P_9\},\$	$\{P_6, P_8, P_9, P_{10}\},\$
	$\{P_3, P_5, P_9, P_{10}\},\$	$\{P_2, P_5, P_6, P_7\},\$
($\{P_4, P_5, P_6, P_{10}\},\$	$\{P_2, P_4, P_6, P_9\},\$
$\{P_1, P_2, P_4, P_7\},\$	$\{P_1, P_2, P_5, P_{10}\},\$	$\{P_3, P_4, P_8, P_9\},\$
$\{P_2, P_3, P_6, P_{10}\},\$	$\{P_1, P_5, P_6, P_9\},\$	$\{P_3, P_5, P_6, P_8\},\$
$\{P_4, P_6, P_7, P_8\},\$	$\{P_5, P_7, P_8, P_{10}\},\$	$\{P_1, P_6, P_7, P_{10}\},\$
$\{P_3, P_4, P_7, P_{10}\},\$	$\{P_1, P_4, P_5, P_8\},\$	$\{P_2, P_4, P_8, P_{10}\},\$
$\{P_1, P_2, P_6, P_8\},\$	$\{P_1, P_4, P_9, P_{10}\},\$	$\{P_1, P_7, P_8, P_9\},\$
$\{P_2, P_3, P_7, P_8\},\$	$\{P_2, P_5, P_8, P_9\},\$	$\{P_1, P_3, P_8, P_{10}\},\$
$\{P_2, P_3, P_4, P_5\},\$	$\{P_1, P_3, P_5, P_7\},\$	$\{P_1, P_3, P_4, P_6\}.$

- \mathcal{E}' and \mathcal{E} admit the same automorphism group $G = \text{PGO}^-(4, q)$ which acts transitively on the plane sections of \mathcal{E} .
- S is the so-called Witt design W_{10} ;
- The isomorphism group of S is denoted by M_{10} and is isomorphic to a proper subgroup of PGL(2, 9) containing PSL(2, 9).
- G in its 6-dimensional representation is reducible; it fixes a line ℓ which is splitted into two orbits:

$$\ell_1 = \{ (1, 1, 0, 2, 2, 2), (1, 2, 2, 0, 1, 2) \}; \\ \ell_2 = \{ (1, 0, 1, 1, 0, 2), (0, 1, 2, 1, 2, 0) \}.$$

Fix the orbit ℓ_1 and let $\mathcal{E}_1 = \mathcal{E}' \cup \{(1, 1, 0, 2, 2, 2)\}$. Then, \mathcal{E}_1 turns out to be the set of points of the unique Steiner system S(4, 5, 11) admitting M_{11} as its automorphism group. The cap code associated to \mathcal{E}_1 is the well known ternary Golay code, which is a perfect $[11, 6, 5]_3$ code, see [8, 20, 21].

Further, let $\mathcal{E}_2 = \mathcal{E}_1 \cup \{(1, 2, 2, 0, 1, 2)\}$. Then, \mathcal{E}_2 turns out to be the set of points of the unique Steiner system S(5, 6, 12) admitting M_{12} as its automorphism group, see [8, 21]. We obtained the following result.

LEMMA 4.1. The Gale transform of an elliptic quadric of PG(3,3) can be extended in PG(5,3) to obtain the extended ternary Golay code.

Note that the above procedure can also be applied starting off with the points of the affine plane AG(2,3) obtained by removing from PG(2,3) the line of equation $X_1 + X_2 + X_3 = 0$ —in place of the points of \mathcal{E} —to obtain a cap admitting M_{12} as its automorphism group.

REMARK 4.2. A similar construction can be performed starting off with an hyperbolic quadric in PG(3,3) instead. In this case we end up with a 16cap in PG(11,3) which is the join of four normal rational curves. Furthermore, this 16-cap admits an automorphism group which is isomorphic to the group $PGL(2,3) \times PGL(2,3)$ of the initial hyperbolic quadric.

5 – Extending scalars

In connection with what we have seen in the previous section, it is also interesting to note the following constructions based on the action of the groups M_{11} and M_{12} .

$5.1 - A [110, 5, 90]_9$ -linear code [9]

Start off with a Singer cyclic subgroup S of PSL(5,3). The group S admits a subgroup of order 11 partitioning PG(4,3) into 11-caps. Let \mathcal{K} be one of these caps. Then, \mathcal{K} is the smallest complete cap in PG(4,3), and it is preserved setwise by the Mathieu group M_{11} , see [20]. As we mentioned before, the cap code associated to \mathcal{K} is the well known ternary Golay code.

Embed $\Sigma = PG(4,3)$ in PG(4,9) as a canonical Baer subgeometry, and look at the orbits of M_{11} on PG(4,9) $\setminus \Sigma$; it turns out that M_{11} has five orbits in PG(4,9) of lengths 110, 220, 990, 1980 and 3960.

Recall that \mathcal{K} has 55 secants; let r be an arbitrary GF(9)-extended secant to \mathcal{K} . The stabilizer H of r in M_{11} is the group

$$M_9 \rtimes C_2 \simeq (E_9 \times Q_8) \rtimes C_2$$

of order 144.

Now let \mathcal{O} be the orbit of size 110 in $\mathrm{PG}(4,9) \setminus \Sigma$. The group H has four orbits on r: three of them have length 2, while the fourth one has length 4. Two of the orbits of length 2 yield the line $r \cap \Sigma$. Varying r among the secants to \mathcal{K} , the other orbit of length 2 gives rise to the orbit \mathcal{O} we mentioned before. Actually, \mathcal{O} is a complete 110-cap of $\mathrm{PG}(4,9)$.

The 110-cap \mathcal{O} yields a $[110, 5, 90]_9$ -linear code C with weight distribution

$$2^{55}, 8^{1980}, 11^{1320}, 14^{2970}, 17^{990}, 20^{66}$$

A code with the same parameters can be found in [1]. However, in the cited paper the authors do not mention its automorphism group. The main advantage of our approach relies on the fact that it is possible to keep track of the automorphism group throughout the construction procedure, and codes with large automorphism groups are of some interest in their own right. 5.2 – A [132, 6, 96]₉-linear code

The extended ternary Golay code is a $[12, 6, 6]_3$ linear code obtained by adding a zero-sum check digit to the $[11, 6, 5]_3$ code. The automorphism group of the extended ternary Golay code is $C_2 \times M_{12}$. Such a code can be realized geometrically in terms of a 12-cap C in PG(5,3), see [10].

Embed $\Pi = PG(5,3)$ in PG(5,9) as a canonical Baer subgeometry and look at the orbits of $G = M_{12}$ on $PG(5,9) \setminus \Pi$. With the aid of MAGMA [2] we checked that G has one orbit \mathcal{O} of size 132 which is a cap.

The number of secants to C is 66. Let r be an arbitrary \mathbb{F}_9 -extended secant to C. The stabiliser H of r in G is the group

$$M_{10} \rtimes C_2 \simeq A_6 \times E_4$$

of order 1440. The group H has 4 orbits on r of lenghts 2, 2, 2 and 4.

Two orbits of length 2 form the the line $r \cap \Pi$. Varying r among the secants to C, the remaining orbit of size 2 gives rise to the cap O. Therefore, Coxeter's 12-cap gives rise to our cap O. We checked with MAGMA [2] that the cap-code arising from O is a [132, 6, 96]₉ linear code.

REFERENCES

- [1] J. BIERBRAUER T. A. GULLIVER: New linear codes over \mathbf{F}_9 , Australas. J. Combin. **21** (2000) pp. 131–140.
- [2] W. BOSMA J. J. CANNON C. PLAYOUST: The Magma algebra system. I. The user language, J. Symbolic Comput. 24,3-4 (1997) pp. 235–265.
- [3] G. CASTELNUOVO: Su certi gruppi associati di punti, Rend. Circ. Mat. Palermo 3 (1889) pp. 179–192.
- [4] A. B. COBLE: Point sets and allied Cremona groups. I, Trans. Amer. Math. Soc. 16, 2 (1915) pp. 155–198.
- [5] A. B. COBLE: Point sets and allied Cremona groups. II, Trans. Amer. Math. Soc. 17, 3 (1916) pp. 345–385.
- [6] A. B. COBLE: Point sets and allied Cremona groups. III, Trans. Amer. Math. Soc. 18, 3 (1917) pp. 331–372.
- [7] A. B. COBLE: Associated sets of points, Trans. Amer. Math. Soc. 24, 1 (1922) pp. 1–20.
- [8] A. COSSIDENTE A. SONNINO: Finite geometry and the Gale transform, To appear on Discrete Math., doi:10.1016/j.disc.2009.08.019.
- [9] A. COSSIDENTE A. SONNINO: A geometric construction of a $[110, 5, 90]_9$ -linear code admitting the Mathieu group M_{11} , IEEE Trans. Inform. Theory 54, 11 (2008) pp. 5251–5252.
- [10] H. S. M. COXETER: Twelve points in PG(5, 3) with 95040 self-transformations, Proc. Roy. Soc. London. Ser. A 247 (1958) pp. 279–293.

- [11] H. DOBRINER: Über das Räumliche Achteck welches die Schnittpunkte dreier Oberflächen zweiter Ordnung bilden, Acta Math. 12 (1889) pp. 339–361.
- [12] D. EISENBUD S. POPESCU: The projective geometry of the Gale transform, J. Algebra 230, 1 (2000), pp. 127–173.
- [13] F. FLAMINI: Towards an inductive construction of self-associated sets of points, Matematiche (Catania) 53 (1998), no. suppl., pp. 33–41 (1999), Pragmatic 1997 (Catania).
- [14] D. GALE: Neighboring vertices on a convex polyhedron, Linear inequalities and related system, Annals of Mathematics Studies, Princeton University Press, Princeton, N.J., 38 (1956) pp. 255–263.
- [15] V. D. GOPPA: A new class of linear correcting codes, Problemy Peredaci Informacii 6, 3 (1970) pp. 24–30.
- [16] V. D. GOPPA: Codes and information, Uspekhi Mat. Nauk 39, 1(235) (1984) pp. 77–120.
- [17] L. O. HESSE: De curvis et superficiebus secundi ordinis, J. Reine Angew. Math. 20 (1840) pp. 285–308.
- [18] L. O. HESSE: Über die lineare Construction des achten Schnittpunktes dreier Oberflächen zewiter Ordnung, wenn sieben Schnittpunkte derselben gegeben sind, J. Reine Angew. Math. 26 (1840) pp. 147–154.
- [19] J. W. P. HIRSCHFELD J. A. THAS: General Galois geometries, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1991.
- [20] G. PELLEGRINO: Sulle proprietà della 11-calotta completa di S_{4,3} e su un B.I.B.disegno ad essa collegato, Boll. Un. Mat. Ital. 7, 4 (1973) pp. 463–470.
- [21] G. PELLEGRINO: Su una interpretazione geometrica dei gruppi M_{11} ed M_{12} di Mathieu e su alcuni $t - (v, k, \lambda)$ -disegni-deducibili da una $(12)_{5,3}^{4}$ calotta completa, Atti Sem. Mat. Fis. Univ. Modena **23**, 1 (1974) pp. 103–117 (1975).
- [22] J. ROSANES: Über linear abhängige Punktsysteme, J. Reine Angew. Math. 88 (1880) pp. 241–272.
- [23] J. ROSANES: Zur Theorie der reciproken Verwandshaften, J. Reine Angew. Math. 90 (1881) pp. 303–321.
- [24] D. J. STRUIK (ed.): A source book in mathematics, 1200–1800, Princeton Paperbacks, Princeton University Press, Princeton, NJ, 1986, Reprint of the 1969 edition.
- [25] R. STURM: Uber Collineation und Correlation, Math. Ann. 12 (1877) pp. 254–368.
- [26] G. K. C. VON STAUDT: Beiträge zur Geometrie der Lage, vol. 3, Verlag von Bauer und Raspe (Julius Merz), Nürnberg, 1860.
- [27] T. WEDDLE: On the theorems in space analogous to those of Pascal and Brianchon in a plane, Cambridge and Dublin Math. J. 5 (1852) pp. 58–69.
- [28] H. WHITNEY: Some combinatorial properties of complexes, Proc. Nat. Acad. Sci. U. S. A. 26 (1940) pp. 143–148.

[29] H. G. ZEUTHEN: Note sur les huit points d'intersection de trois surfaces du second ordre, Acta Math. 12 (1889) pp. 362–366.

> Lavoro pervenuto alla redazione il 10 marzo 2010 ed accettato per la pubblicazione il 15 marzo 2010. Bozze licenziate il 20 aprile 2010

INDIRIZZO DEGLI AUTORI:

Antonio Cossidente – Dipartimento di Matematica e Informatica – Università della Basilicata – Campus Macchia Romana – Viale dell'Ateneo Lucano, 10 – 85100 Potenza, Italy E-mail: antonio.cossidente@unibas.it

Angelo Sonnino – Dipartimento di Matematica e Informatica – Università della Basilicata – Campus Macchia Romana – Viale dell'Ateneo Lucano, 10 – 85100 Potenza, Italy E-mail: angelo.sonnino@unibas.it