IEEE Pacific Rim Conference on Communications, Computers and Signal Processing
June 1st - 2nd, 1989

SPURIOUS GALOIS FIELDS

Czesław Kościelny

Institute of Engineering Cybernetics
Technical University of Wrocław
27 Wyb. Wyspiańskiego Street
50-370 Wrocław
Poland

Abstract: The algebraic system consisting of finite set of elements with two internal operations of addition and multiplication has been studied. For the above system which satisfies all the axioms of the fields except for the axiom of associativity, which may, but need not be satisfied, the name spurious Galois field and the symbol SGF(q) has been proposed. Such an approach has allowed to show that the spurious Galois fields form a class of algebraic systems containing all the isomorphic Galois fields as its smaller subclass. Some properties of SGF(q) have been presented and some domains of their applications also pointed out. The author follows the notation commonly used in coding theory [2], [4].

I. Introduction

The idea of the spurious Galois fields has appeared in the context of software implementation of computing in finite fields using the Zech's logarithm: it turned out that the program realizing addition in GF(q) also works after replacing the Zech's logarithm by another similar function, giving unpredictable results. Thus the plan of the paper is as follows: section II contains the definition of spurious Galois fields, section III gives the rules of computing in SGF(q), and defines conditions which could allow the GF(q) to be spurious, section IV describes some properties of SGF(q), and section V shows how to solve the problem of software implementation of operations in SGF(q) to obtain the useful tool for studying the properties of the spurious Galois fields.

II. Definition of spurious Galois fields

Let

$$\langle SF,+,\cdot\rangle \tag{1}$$

be an algebraic system consisting of non-empty, finite set of elements in which two internal binary operations called addition and multiplication respectively, are defined and let

card $SF=q$, $q=p^m$, p-prime, m-positive integer ≥ 1

be satisfied.

The spurious Galois field, denoted by SGF(q), is the system (1), satisfying the axioms:

S.1. $\exists\ 0 \in SF\ \forall\ a \in SF\ a+0=0+a=a$,

S.2. $\forall\ a \in SF\ \exists\ -a \in SF\ a+(-a)=(-a)+a=0$,

S.3. $\forall$ a, b SF $a+b=b+a$,

S.4. $\exists\ -1 \in SF\ [-1=1$ if $p=2$
or $-1\ \omega^{(q-1)/2}$ if $p>2]$,

S.5. $\langle SF^{*},\cdot\rangle$ is an abelian multiplicative group, SF^{*} denoting $SF-\{0\}$. This axiom implies that $SF=\{0,1,\omega,\omega^{2},\ldots,\omega^{q-2}\}$, $\omega^{q-1}=1$,

S.6 $\forall$ $a,b,c \in SF$ $[a.(b+c)=a.b+a.c]$
$\&[(b+c).a=b.a+c.a]$.

III. Computation in SGF(q)

Let $Q=\{0,1,\ldots,q-2\}$. From the axioms S.5. and S.6 it follows that multiplicative operations can be concisely described using the formulae

$$\forall\ r,s \in Q\quad \omega^{r}.\omega^{s}=\omega^{r+s(\mathrm{mod} q-1)}, \tag{2}$$

$$\forall\ r \in Q\ \omega^{-r}=1/\omega^{r}=\omega^{q-1-r}, \tag{3}$$

$$\forall\ r,k \in Q\quad (\omega^{r})^{k}=\omega^{rk\ (\mathrm{mod}\ q-1)}, \tag{4}$$

$$\forall\ r \in Q\ \omega^{r}.0=0. \tag{5}$$

To perform addition in SGF(q) one must know the discrete implicite function

$$\omega^{SZ(x)}=1+\omega^{x} \tag{6}$$

defined on the set $\{-\infty,0,1,\ldots,q-2\}$ and taking the values from this set. Here, the symbol $-\infty$ denotes an element of the set different from the other elements; this symbol is used to express $\omega^{-\infty}=0$.

Then $1+\omega^{-\infty}=\omega^{0}$ giving

$$SZ(-\infty)=0\quad \text{for } p\geq 2. \tag{7}$$

By the axiom S.4 we get

$$SZ(0)=-\infty\quad \text{if } p=2, \tag{8}$$

$$SZ[(q-1)/2]=-\infty \text{ if } p>2. \tag{9}$$

The values of the function $SZ(x)$ for $x\neq-\infty$, $x\neq0$ if $p=2$ and $x\neq(q-1)/2$ if $p>2$ must all be different but they can be chosen arbitrarily so as to satisfy the condition

$$SZ(x)\neq x \tag{10}$$

because there is only one identity element of the groupoid $\langle SF,+\rangle$.

It should be noted that the function $SZ(x)$ fully determines the properties of the groupoid. It is proposed to name the function $SZ(x)$ spurious Zech's logarithm.

Additive operations are performed according to the relations

$$\forall\ r \in Q \quad -\omega^r = \begin{cases} \omega^r \text{ if } p=2, \\ \omega^{r+(q-1)/2 \ (\mathrm{mod}\ q-1)} \text{ if } p>2, \end{cases} \qquad (11)$$

$$\forall\ r,s \in Q \ \ \omega^r+\omega^s = \begin{cases} 0 \text{ if } SZ|r-s|=-\infty, \\ \omega^r \text{ if } \omega^s=0, \\ \omega^s \text{ if } \omega^r=0, \\ \omega^{\min(r,s)+SZ|r-s| (\mathrm{mod}\ q-1)} \\ \text{if } \omega^r, \omega^s \neq 0 \text{ and } SZ|r-s| \neq -\infty. \end{cases} \qquad (12)$$

IV. Some properties of SGF(q)

To calculate the number of all possible SGF(q)'s it is necessary, with (7)÷(10) satisfied, to solve relatively simple combinatorial problem. Its solution is as follows:

$$ns(q) = \begin{cases} (q-2)! \sum_{k=2}^{q-2} (-1)^k/k! \text{ if } p=2, \\ (q-3)! \sum_{k=0}^{q-3} (-1)^k (q-2-k)/k! \text{ if } p>2, \end{cases} \qquad (13)$$

ns(q) denoting the number of all possible SGF(q)'s. Table I was calculated using this formula for the first 18 values of q.

Table I

q	ns(q)
2	1
3	1
4	1
5	3
7	53
8	265
9	2119
11	148329
13	16019531
16	32071101049
17	513137616783
19	138547156531409
23	19690321886243846661
25	9923922230666898717143
27	5934505493938805432851513
29	41541538457571638029960590099
31	33648646150633026804268078701 89
32	9758107383683577773237742823 5481

It is thus possible to construct ns(q) different SGF(q)'s. Among them there are all the isomorphic GF(q)'s. For a given q the multiplication table is the same for all SGF(q), each SGF(q) having a different addition table. The distribution of SGF(q) elements in the addition table can be very various, but all the addition tables are symmetrical relative to the diagonal, because the groupoid <SF,+> is commutative.

Generally, addition in SGF(q) is not an associative operation except for SZ(x)=Z(x), namely, if SZ(x) becomes the Zech's logarithm. However, there exist SGF(q)'s containing a subset of elements for which addition is associative. This subset is formed by one or more subfields of GF(q) "implanted" into SGF(q).

It has been observed that for q>5, for a certain number of SGF(q)'s, which are not GF(q)'s, the addition tables have a form of latin square. These SGF(q)'s, further called latin square SGF(q)'s, seem to be most interesting for applications.

Although addition in the latin square SGF(q) with SZ(x)≠Z(x) is not associative, the equations

$$a+x=b, \ \ y+a=b \qquad (14)$$

have the unique solution for each pair a,b∈SF, because in this case the groupoid <SF,+> becomes a quasi-group.

It has been noted that each latin square SGF(q) satisfies the condition

$$SZ(x) \equiv SZ(q-1-x)+x \ (\mathrm{mod}\ q-1). \qquad (15)$$

Taking into account (15) it can be easily proved that for p>2

$$SZ(0) \equiv [(5q-11)(q-1)]/8 \ (\mathrm{mod}\ 2). \qquad (16)$$

Let now β be a generator of $\langle SF^*, \cdot \rangle$, then $\beta=\omega^k$, $(k,q-1)=1$ and

$$\beta^{SZ'(x)}=1+\beta^x \Rightarrow \omega^{kx}+1=\omega^{kSZ'(x)}=\omega^{SZ(kx)}.$$

Therefore

$$kSZ'(x) \equiv SZ[kx(\mathrm{mod}\ q-1)] \ (\mathrm{mod}\ q-1) \qquad (17)$$

Thus knowing SZ(x) for one latin square SGF(q) it is possible to calculate other functions SZ'(x) determining up to $[\varphi(q-1)]/m$ new latin square spurious Galois fields, $\varphi(.)$ denoting the Euler's function.

The formulae (15)÷(17) can considerably simplify the work of finding all the latin square SGF(q)'s.

To calculate the number of all possible latin square SGF(q)'s one must attack the problem much more complicated than the latter in calculating ns(q). However, table II estimates this number. It should be noted that all the GF(q)'s belong to the ensemble of latin square SGF(q)'s.

Table II.

q	number of latin square SGF(q)	number of isomorphic GF(q)
2	1	1
3	1	1
4	1	1
5	2	2
7	4	2
8	3	2
9	12	2
11	56	4
13	224	4
16	631	2
17	$c.10^3$	8
19	$c.10^4$	6
23	$c.10^5$	10
25	$c.10^5$	4
27	$c.10^6$	4
29	$c.10^7$	12
31	$c.10^7$	8
32	$c.10^8$	6

$c \in [1,100]$

Frankly speaking it is difficult to state with full certainty that the coefficient c was chosen properly.

V. Software approach to computing in SGF(q)

The easiest way to implement operations in SGF(q) is to replace the abstract representation of elements of SGF(q) by the set of integers

$$F=\{0,1,\dots,q-1\} \tag{18}$$

and to apply the bijective mapping

$$T : SF \to F \tag{19}$$

defined by the function

$$T(\omega^{x})=\begin{cases} x+1 \text{ if } \omega^{x}\neq 0, \\ 0 \text{ if } \omega^{x}=0. \end{cases} \tag{20}$$

It can be verified that

$$\forall\, a,b \in SF\ [T(a.b)=T(a)\underset{\vee}{\cdot}T(b)]$$
$$\&[T(a+b)=T(a)\overset{\wedge}{\underset{\vee}{+}}T(b)]. \tag{21}$$

Therefore the mapping T is an isomorphism, and this being so, there exists the inverse mapping

$$T^{-1} : F \to SF \tag{22}$$

$$T^{-1}(x)=\begin{cases} \omega^{x-1} \text{ if } x>0, \\ 0 \text{ if } x=0. \end{cases} \tag{23}$$

In this way the operations in SGF(q) can be transformed into simple arithmetic operations on integers.

For almost all applications it is sufficient to define five functions realizing the product, k-th power, sum, multiplicative inverse and additive inverse of elements of SGF(q), denoted respectively P(x,y), PR(x,k), S(x,y), MI(x), AI(x) and expressed as follows

$$P(x,y)=T(\omega^{x-1}.\omega^{y-1}), \tag{24}$$

$$PR(x,k)=T[\omega^{(x-1).k}], \tag{25}$$

$$S(x,y)=T(\omega^{x-1}+\omega^{y-1}), \tag{26}$$

$$MI(x)=T(1/\omega^{x-1}), \tag{27}$$

$$AI(x)=T(-\omega^{x-1}). \tag{28}$$

Taking into account (2)÷(12) and (18)÷(28) one obtains immediately

$$P(x,y)=\begin{cases} 1+[x+y-2 \pmod{q-1}] \text{ if } x,y>0, \\ 0 \text{ if } x=0 \text{ or } y=0, \end{cases} \tag{29}$$

$$PR(x,k)=\begin{cases} 1+[(x-1).k \pmod{q-1}) \text{ if } x>0, \\ 0 \text{ if } x=0, \end{cases} \tag{30}$$

$$MI(x)=\begin{cases} q+1-x \text{ if } x>1, \\ 1 \text{ if } x=1, \end{cases} \tag{31}$$

$$AI(x)=\begin{cases} x+(q-1)/2 \pmod{q-1} \\ \qquad \text{if } x\neq 0 \text{ and } p>2, \\ x \text{ if } x\neq 0 \text{ and } p=2, \\ 0 \text{ if } x=0, \end{cases} \tag{32}$$

$$S(x,y)=\begin{cases} 1+[\min\{x,y\}+SZ|x-y|-1 \pmod{q-1}] \\ \qquad \text{if } x,y\neq 0 \text{ and } SZ|x-y|\neq -\infty, \\ \max\{x,y\} \text{ if } x=0 \text{ or } y=0, \\ 0 \qquad \text{if } SZ|x-y|=-\infty. \end{cases} \tag{33}$$

The formulae (29)÷(33) can be easily written down in any high-level programming language.

Conclusion

It can be hoped that the spurious Galois fields can find some applications in the discrete mathematics, coding theory and algebraic theory of automata. The existence of a great number of latin square SGF(q)'s for sufficiently great q seems to be interesting for cryptography [1]. In some domains one can also use the "linear recurring relations" over SGF(q), generating the periodic sequences having the properties different from those over GF(q) [3].

It is also noteworthy to say that the software based upon the formulae (29)÷(33) is universal, namely, it can be used to compute in SGF(q), GF(q) and GF(p) as well. It has been practically verified that this software is a useful tool for implementation of coding and decoding procedures of generalized cyclic codes.

References

[1] Cz. Kościelny, A cryptographic procedure using latin square spurious Galois fields, to be presented at the conference on performance evaluation, reliability and exploitation of computer systems "RELCOMEX'89", Książ Castle, 26÷29.09.1989, Poland.

[2] F. J. MacWilliams, N. J. A. Sloane, The theory of error-correctig codes, Amsterdam, North Holland 1977.

[3] W. Mochnacki, An application of periodic sequences over SGF(q) in cryptography, to be presented at "RELCOMEX'89" conference.

[4] W. W. Peterson, E. J. Weldon Jr., Error-correcting codes, MIT Press 1972.