Publ. Math. Debrecen
58 / 3 (2001), 441–449

On a conditional Cauchy functional equation involving cubes of finite fields III: The case of characteristic 2

By J-L. GARCÍA-ROIG (Barcelona)
and EMMA MARTÍN-GUTIÉRREZ (La Coruña)

Abstract. We solve the conditional Cauchy functional equation $f(x^3+y^3) = f(x^3)+f(y^3)$, where f is a map from a finite field of characteristic 2 into itself.

1. Introduction

In this paper we solve the conditional Cauchy functional equation

$$f(x^3+y^3) = f(x^3)+f(y^3) \tag{1}$$

where f is a map from a finite field $\mathbb{F}_q$, where $q=2^n$, into itself.

This completes our study of functional equation (1) for maps from a finite field into itself, which has been considered earlier in [G–M 1] and [G–M 2] (the case $q=3^n$ is contained in Remark 3 on p. 395 of [G–M 1]). In the present situation there appear two exceptional cases whose solutions differ from those of the usual Cauchy functional equation. This is not surprising, for we have already encountered three exceptional cases in [G–M 1].

2. The functional equation $f(x^3+y^3) = f(x^3)+f(y^3)$ for maps $f:\mathbb{F}_q\to\mathbb{F}_q$, with $q=2^n$

The case n odd can be treated as in Lemma 1 of [G–M 2], which holds in our present case. Essentially the same proof is valid, with the

Mathematics Subject Classification: 39B52.
Key words and phrases: functional equation, Cauchy functional equation, finite field.

simplification that the quadratic form X^2+XY+Y^2 or, equivalently, the polynomial X^2+X+1, is obviously irreducible over $\mathbb{F}_{2^n}$ if and only if n is odd (neither 0 nor 1 is a root of the latter polynomial, so that its roots are precisely the elements of $\mathbb{F}_4$ not in $\mathbb{F}_2$).

Thus, as in [G–M 2], for n odd, functional equation (1), for maps $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, is equivalent to the Cauchy functional equation, and we will assume in the sequel that n is even.

This remaining case will be treated following the pattern of our two earlier papers [G–M 1] and [G–M 2]: any map $f : \mathbb{F}_q \to \mathbb{F}_q$ is induced by a (reduced) polynomial

$$P(T) = a_0 + a_1T + a_2T^2 + \cdots + a_{q-1}T^{q-1} \tag{2}$$

with $a_0, a_1, \ldots, a_{q-1}$ in $\mathbb{F}_q$. Condition (1) entails that the mixed terms of the reduction (via $T^q \equiv T$) of $P(X^3+Y^3)$ vanish and this leads to the linear system of equations on the coefficients of $P(T)$:

$$E_r^j = 0, \quad \text{with} \quad k < j \le 2k \quad \text{and} \quad 0 < r \le \left[\frac{j}{2}\right], \tag{3}$$

where $k = \frac{1}{3}(2^n - 1)$ (which makes sense since n is even), $\left[\frac{j}{2}\right]$ is the integral part of $\frac{j}{2}$, and E_r^j stands for

$$\binom{j-k}{r}a_{j-k} + \left[\binom{j}{r} + \binom{j}{r+k}\right] a_j$$
$$+ \left[\binom{j+k}{r} + \binom{j+k}{r+k} + \binom{j+k}{r+2k}\right] a_{j+k} = 0,$$

if $\binom{j}{r}$ lies outside triangle ABC (see the figure), and for

$$\binom{j}{r}a_j + \left[\binom{j+k}{r} + \binom{j+k}{r+k}\right] a_{j+k} = 0,$$

if $\binom{j}{r}$ lies either inside triangle ABC or on its side AC.

3. The arithmetic triangle modulo 2 in connection with (3) for even powers of 2

In this section we will always assume that the degree n of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is even and $(a_2, a_3, \ldots, a_{3k})$ will stand for an arbitrary solution of the

Figure 1.

linear system of equations (3). As in [G–M 1] and [G–M 2] we have (cf. [H] or [L])

$$\binom{j}{r} \equiv \prod_{i=0}^{n-1} \binom{j_i}{r_i} \pmod 2 \tag{4}$$

where j_i and r_i stand for the digits occurring in the respective binary expansions $(j_{n-1}, \dots, j_0)$ and $(r_{n-1}, \dots, r_0)$ of j and r (both supposed to have at most n binary digits and where, of course, we assume $\binom{0}{1} = 0$).

Letting $k = \frac{2^n-1}{3}$, as in the previous section, we easily have the following binary expansions (of n digits, written from right to left, as usual):

$$k = (0, 1, 0, 1, \dots, 0, 1),$$

$$2k = (1, 0, 1, 0, \dots, 1, 0).$$

These expressions immediately (by (4)) entail that vertex $C = \binom{2k}{k} \equiv 0 \pmod 2$, as in [G–M 2]. On the other hand, the equality $(a+b)^{2^r} = a^{2^r} + b^{2^r}$ in characteristic 2 implies that the inverted triangle $A'B'C'$ below the 2^{n-1}th row is a null triangle modulo 2 (except for its slanting sides which consist of ones). Furthermore, from $3k = 2^n - 1 = (1, 1, \dots, 1)$, we easily get $E = \binom{3k}{k} \not\equiv 0 \pmod 2$, and proceeding as in [G–M 1] Lemma 3, we have

Lemma 1. *For each j, with $k < j < 2k$, there exists at least an r, with $j - k \leq r \leq k$, such that*

$$\binom{j+k}{r} + \binom{j+k}{j-r} \not\equiv 0 \qquad (\mathrm{mod}\ 2).$$

Remark. The preceding lemma does not hold for $j = 2k$, as was the case in our previous papers. In fact, here we have $\binom{3k}{k} + \binom{3k}{2k} \equiv 2 \equiv 0$ (mod 2).

Now, reasoning as in Proposition 6 of [G–M 2], we get the following.

Proposition 2. *We have:*

i) *if $a_{j+k} = 0$, for some j, with $k < j < 2^{n-1}$, then $a_j = 0$,*

ii) *if $a_j = 0$, for some j, with $k < j < 2k$, then $a_{j+k} = 0$.*

Again, reasoning as in Proposition 1 of [G–M 1], we get

Proposition 3. *For any j, with $k < j \leq 2k$, if $a_j = a_{j+k} = 0$, then:*

$$\begin{aligned} &a_{j-k} = 0, && \textit{if} \quad j - k \neq 2^m, \\ &a_{j-k} \textit{ is arbitrary}, && \textit{if} \quad j - k = 2^m. \end{aligned}$$

Remark. The above assertion differs from that of Proposition 1 of [G–M 1]: the reason is that here (as will soon be seen) it is not true that $a_j = 0$, for $j = k + 1, \ldots, 3k$.

We will tackle the study of the system of equations (3) by first treating the cases $j = 2^{n-1}$ and $j = 2k$, for $n \geq 6$. As there arise some particularities for $n = 2$ and 4, we postpone the complete study of these cases to the end of this section. The following lemmas refer to solutions of (3).

Lemma 4. *For even $n \geq 4$, we have $a_{2^{n-1}-k} = a_{2^{n-1}+k} = 0$, but $a_{2^{n-1}}$ is arbitrary.*

Proof. We have already mentioned that the 2^{n-1}th row (without endpoints) consists of zeros, so that no condition at all is imposed on $a_{2^{n-1}}$. The rest is a consequence of Lemma 1 (which can be applied since, for $n > 2$, $2^{n-1} < 2k$): equation $E_r^{2^{n-1}} = 0$, for the r quoted in that lemma, yields $a_{2^{n-1}+k} = 0$, and now, for instance, from equation $E_1^{2^{n-1}} = 0$ we see that $a_{2^{n-1}-k} = 0$. □

Lemma 5. *For even $n \geq 6$, we have $a_k = a_{2k} = a_{3k} = 0$.*

Proof. It suffices to consider the equations associated with $\binom{2k}{1}$, $\binom{2k}{2}$ and $\binom{2k}{3}$. Bearing in mind that

$$\binom{2k}{3+k} \equiv \dots \binom{1}{0}\binom{0}{1}\binom{1}{1}\binom{0}{0}\binom{1}{0}\binom{0}{0} \pmod 2$$

is congruent with zero (mod 2), since $n \geq 6$, the determinant of this subsystem is easily seen to be congruent with 1 and thus, $a_k = a_{2k} = a_{3k} = 0$. □

Lemma 6. *For even n, we have $a_j = a_{j+k} = 0$, for those j such that $2^{n-1} < j < 2k$.*

Proof. We can assume $n > 2$ (for $n = 2$, $2^{n-1} = 2k$). On the other hand, by Proposition 2 (ii), it suffices to show that $a_j = 0$ in order to get $a_{j+k} = 0$, but it turns out that, for $2^{n-1} < j < 2k$, it is immediately seen that $a_{j+k} = 0$ (just consider the equation $E^j_r = 0$, for the r appearing in Lemma 1, and observe that $\binom{j}{r} \equiv 0 \pmod 2$ since it lies inside triangle $A'B'C'$).

In order to prove that $a_j = 0$, observe that, as

$$2^{n-1} = (1,0,0,0,\dots,0,0) < j < (1,0,1,0,\dots,1,0) = 2k,$$

j has to be of type: $(1,0,0,0,\dots),(1,0,0,1,\dots)$ or $(1,0,1,0,\dots)$. When $j = (1,0,1,0,\dots)$ (which cannot occur if $n = 4$, since $j < 2k$), equation $E^j_r = 0$, with $r = (0,0,1,0,\dots,0,0)$, yields $a_j = 0$. When $j = (1,0,0,1,\dots)$, we have $j - k = (0,1,0,0,\dots)$ or $(0,0,1,1,\dots)$. In the first case $E^j_r = 0$, with $r = (0,0,0,1,0,\dots,0)$, yields $a_j = 0$. This also holds in the second case, but after having seen that $E^j_s = 0$, with $s = (0,0,1,0,\dots)$, entails $a_{j-k} = 0$.

When $j = (1,0,0,0,\dots)$ equation $E^j_r = 0$, with $r = (0,0,1,0,\dots,0)$, yields $a_{j-k} = 0$. On the other hand, as we can assume to work with at least 6 digits (this case does not occur for $n = 4$, since $j > 2^{n-1}$), to the right of the first four digits of j, there appears at least a one (since $j > 2^{n-1}$), say corresponding to the place of power 2^t.

Then equation $E^j_s = 0$, with $s = 2^t$, entails $a_j = 0$. □

Lemma 7. *For even $n \geq 4$, we have $a_j = a_{j+k} = 0$, for those j such that $k < j < 2^{n-1}$.*

Proof. By Proposition 2, it suffices to prove that either $a_j = 0$ or $a_{j+k} = 0$, for each j, $k < j < 2^{n-1}$.

Let us begin by considering the cases $j = k+1$, $k+2$: $E_1^{k+1} = 0$ yields $a_{2k+1} = 0$, and $E_2^{k+2} = 0$, $a_{k+2} = 0$. These cases exhaust all possibilities when $n = 4$, so that in the rest of the proof we will assume $n \geq 6$ and, consequently, the binary expansion of k will contain at least 3 couples (0,1). As $k < j < 2^{n-1}$, the binary expansion of j consists of a couple (0,1) on the left, then there may be more of these couples but, on going to the right, we eventually get a place where a 0 has been replaced by a 1. Except for the cases $k+1$ and $k+2$ (solved above), where after the last couple (0,1) there appear two digits, in the remaining cases, after the last couple (0,1) there are at least four digits, which we can denote as

$$j = (\dots, 0, 1, x, y, z, t, \dots)$$

where, on the left of (0,1) there may appear more couples (0,1), and on the right of t there may appear more digits. In any case, the group of digits (x, y, z, t) has to be of one of the following eight types:

a) $1,0,0,0$ *b*) $1,0,0,1$ *c*) $1,0,1,0$ *d*) $1,0,1,1$

e) $1,1,0,0$ *f*) $1,1,0,1$ *g*) $1,1,1,0$ *h*) $1,1,1,1$.

In case there appear more digits on the right of t, in adding $j+k$ (from right to left, as usual), we have two possibilities on arriving at the digit t:

1) we carry nothing from previous digits,

2) we carry a unit from previous digits.

There are thus, 16 possible cases. In each one of them, we will choose an r of which we will just indicate its digits corresponding to the places of 0, 1, x, y, z, t in j, with the understanding that the remaining digits are zeros. Now it is immediate that taking $r = (\dots, 0, 0, 1, 0, 1, 0, \dots)$ for (a.2), (b.1), (b.2), (c.2), (d.1), (d.2), (g.1) and (g.2); $r = (\dots, 0, 0, 1, 0, 0, 1, \dots)$ for (a.1), (c.1), (f.1) and (f.2); $r = (\dots, 0, 0, 1, 1, 0, 1, \dots)$ for (h.1) and (h.2); and $r = (\dots, 0, 0, 1, 0, 0, 0, \dots)$ for (e.1) and (e.2), then $\binom{j}{r}$ lies inside triangle ABC, so that exactly 2 of the 3 binomial coefficients occurring in the associated equation are zero: consequently $a_j = 0$ or $a_{j+k} = 0$. □

Proposition 3 together with the four preceding lemmas establish the following.

Theorem 8. *For $q = 2^n$, n even ≥ 6, the solutions $(a_2, a_3, \ldots, a_{3k})$ of (3) are given by*

$$a_t = \begin{cases} 0, & \text{if } t \text{ is not a power of } 2, \\ \text{arbitrary}, & \text{otherwise}, \end{cases}$$

for $2 \leq t \leq 3k$.

Next we include the cases $q = 2^2$ and 2^4.

Theorem 9. *For $q = 2^2$, any couple of elements in $\mathbb{F}_4$ is a solution of (3).*

Proof. (3) reduces in this case to equation $0a_2 + (1+1)a_3 = 0$. □

Theorem 10. *For $q = 2^4$, the solutions $(a_2, a_3, \ldots, a_{15})$ of (3) are given by:*

$$a_j = 0, \quad \text{for} \quad j \neq 2, 4, 5, 8, 10, 15,$$

$$a_{15} = a_{10} = a_5, \qquad \text{and}$$

$$a_2,\ a_{2^2},\ a_{2^3} \text{ and } a_5 \text{ may be arbitrarily chosen.}$$

Proof. By Lemma 4, a_{2^3} is arbitrary and $a_3 = a_{13} = 0$. By Lemmas 6 and 7, $a_9 = a_{14} = 0$, $a_6 = a_{11} = 0$ and $a_7 = a_{12} = 0$ and, consequently, according to Proposition 3, a_2 and a_{2^2} may be arbitrarily chosen. And bearing in mind that the only equations of (3) relating rows k, $2k$ and $3k$ are:

$$\left.\begin{aligned} a_5 + a_{15} &= 0 \\ a_{10} + a_{15} &= 0 \end{aligned}\right\}$$

we conclude that $a_5 = a_{10} = a_{15}$ is arbitrary. □

4. Solutions of functional equation (1) in characterisitic 2

Theorem 11. *The solutions $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ of functional equation (1), for $n \neq 2, 4$, are exactly those of the usual Cauchy functional equation, and may be expressed by the polynomial functions*

$$f(x) = a_1 x + a_2 x^2 + a_{2^2} x^{2^2} + \cdots + a_{2^{n-1}} x^{2^{n-1}}$$

where $a_1, a_2, \dots, a_{2^{n-1}}$ belong to $\mathbb{F}_{2^n}$.

However, for $n = 2$ and 4, there appear more solutions, namely those given by

$$f(x) = a_1x + a_2x^2 + a_3x^3, \qquad \textit{if } n = 2,$$

and

$$f(x) = a_1x + a_2x^2 + a_4x^4 + a_5x^5 + a_8x^8 + a_5x^{10} + a_5x^{15}, \quad \textit{if } n = 4,$$

where the coefficients are assumed to lie in the respective fields $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^4}$.

Proof. The case n odd is immediate, since there exist $(2^n)^n$ solutions of the Cauchy equation (see the beginning of Section 1), so we can assume n even, and f induced by a polynomial of type (2).

By Theorem 8, for $n \geq 6$, any solution f of (1) is actually induced by a polynomial of type

$$P(T) = a_0 + a_1T + a_2T^2 + a_{2^2}T^{2^2} + \cdots + a_{2^{n-1}}T^{2^{n-1}},$$

since the mixed terms of $P(X^3 + Y^3)$ vanish. Now, reducing and equating $P(X^3 + Y^3)$ and $P(X^3) + P(Y^3)$, we obtain $a_0 = 2a_0 = 0$ (observe that the reduction of the only non-reduced terms of $P(X^3 + Y^3)$, namely $a_{2^{n-1}}\big(X^{3\cdot 2^{n-1}} + Y^{3\cdot 2^{n-1}}\big)$ is $a_{2^{n-1}}\big(X^{2^{n-1}+1} + Y^{2^{n-1}+1}\big)$, whose terms do not overlap with the remaining ones), so that the solutions have to be as stated in the theorem. A direct checking shows in fact that these work and we are done.

For the cases $n = 2$ and $n = 4$ we proceed in a similar manner, replacing Theorem 8 by Theorems 9 and 10, respectively, and taking into account the following subtleties:

For $n = 2$, it is convenient to observe that the map $x \mapsto x^3$ sends $\mathbb{F}_4^*$ into 1 (and 0 into 0), so that it satisfies (1).

For $n = 4$, we observe first that the map $\varphi(x) := x^5 + x^{10} + x^{15}$ from $\mathbb{F}_{16}$ into itself takes the value 1 on all nonzero cubes, and 0, otherwise (sum of geometric progression). In order to prove that φ satisfies (1), the only difficulty arises in trying to check (1) for a couple of nonzero distinct elements x, y, for which it suffices to see that $x^3 + y^3$ is not a nonzero cube. This, in turn, is equivalent to seeing $(x^3 + y^3)^5 \neq 1$. Expanding the left-hand side we are led to check that we have $t^3 + t^{-3} \neq 1$, and so, it is enough to prove that $t^6 + t^3 + 1$ does not vanish on any element of $\mathbb{F}_{16}$.

But this follows from the fact that $X^2 + X + 1$ is a defining equation for the extension $\mathbb{F}_2 \subseteq \mathbb{F}_4$, and (because $\mathbb{F}_{4^3} \cap \mathbb{F}_{4^2} = \mathbb{F}_4$) that $X^3 - \alpha$, for any $\alpha \in \mathbb{F}_4 \backslash \mathbb{F}_2$, is irreducible in $\mathbb{F}_4[X]$, since it has degree 3 and no roots in $\mathbb{F}_4$ (alternatively, if there exists β in $\mathbb{F}_{16}$ such that $\beta^3 = \alpha$, then $\alpha^5 = 1$ and as $\alpha^3 = 1$, we get $\alpha^2 = 1$, i.e. $\alpha = 1$, a contradiction). □

References

[G–M 1] J-L. Garcia-Roig and E. Martín-Gutiérrez, On a conditional Cauchy functional equation involving cubes of finite fields I: The case of characteristic $p \equiv 1 \pmod 3$, *Publ. Math. Debrecen* **52**/3–4 (1998), 385–396.

[G–M 2] J-L. Garcia-Roig and E. Martín-Gutiérrez, On a conditional Cauchy functional equation involving cubes of finite fields II: The case of odd characteristic $p \equiv 2 \pmod 3$, *Publ. Math. Debrecen* **55**/1–2 (1999), 101–111.

[H] A. M. Hinz, Pascal's Triangle and the Tower of Hanoi, *Amer. Math. Monthly* (6), **99** (June–July, 1992), 538–544.

[L] E. Lucas, Théorie des Fonctions Numériques Simplement Périodiques, *Amer. J. Math.* **1** (1878), 184–240, 289–321.

J–L. GARCÍA–ROIG
SECCIÓ MATEMÀTIQUES I INF., ETSAB
UNIVERSITAT POLITÈCNICA CATALUNYA
DIAGONAL 649
08028 BARCELONA
SPAIN

EMMA MARTÍN–GUTIÉRREZ
E.T.S. DE ARQUITECTURA DE LA CORUÑA
CAMPUS DE ZAPATEIRA S/N
UNIVERSIDADE DA CORUÑA
15192 LA CORUÑA
SPAIN

(Received July 8, 1999; revised December 16, 1999;
file received May 4, 2000)