On the Structure of Hyperfields Obtained as Quotients of Fields

Matthew Baker and Tong Jin

Abstract. We determine all isomorphism classes of hyperfields of a given finite order which can be obtained as quotients of finite fields of sufficiently large order. Using this result, we determine which hyperfields of order at most 4 are quotients of fields. The main ingredients in the proof are the Weil bounds from number theory and a result from Ramsey theory.

1. Introduction

If $F$ is a field and $G$ is a multiplicative subgroup of $F^\times$, the quotient $F/G$ naturally has the structure of a hyperfield in the sense of M. Krasner; in particular, addition is a multi-valued binary operation. Krasner asked in [Kr83] if every abstract hyperfield arises from this quotient construction; it turns out that the answer is no (the first counterexample was found by Massouros [Ma85]). Nevertheless, it is still of interest to classify quotient hyperfields, and the simplest case is that of quotients of finite fields. In this case, for each $r$ dividing $q - 1$ there is a unique subgroup $G'_q$ of $F_q^\times$ of index $r$, and the quotient $F_q/G'_q$ is a hyperfield of order $r + 1$.

It is natural to fix $r$ and vary $q$ and ask how many different hyperfields of order $r + 1$ one obtains from this construction. For $r = 1$, one always obtains the so-called “Krasner hyperfield” $\mathbb{K}$, and for $r = 2$ it is well-known that when $q \geq 7$ there are just 2 possibilities, depending on whether $q$ is congruent to 1 or 3 modulo 4. (For $q = 3, 5$ one obtains two additional “sporadic” quotient hyperfields of order 3.) Our first main goal in this paper is to generalize these observations to arbitrary natural numbers $r$ (when the prime-power $q$ is sufficiently large). Using the Weil bounds for the number of points on algebraic curves over finite fields, we prove the following:

**Theorem 1.1.** Given an integer $r \geq 2$, there is a bound $N_r$ (which we can take to be $r^4$) such that the following holds:

1. If $r$ is odd, there is a unique hyperfield $\mathbb{H}_r$ such that $F_q/G'_q$ is isomorphic to $\mathbb{H}_r$ for every prime power $q \geq N_r$ with $q \equiv 1 \pmod{r}$.
2. If $r$ is even, there are two distinct hyperfields $\mathbb{H}_r$ and $\mathbb{H}'_r$ such that for every prime power $q \geq N_r$ with $q \equiv 1 \pmod{2r}$ (resp. $q \equiv r + 1 \pmod{2r}$), $F_q/G'_q$ is isomorphic to $\mathbb{H}_r$ (resp. $\mathbb{H}'_r$).

Acknowledgements. We thank Trevor Gunn for catching some typos in the first draft of the paper, and Keith Conrad for historical remarks concerning Theorem 3.1.
Remark 1.2. The proof will show, more precisely, that we can take $N_r$ to be the smallest positive integer $N$ such that $(N + 1) - (r - 1)(r - 2)N^{1/2} - 3r > 0$. When $r = 2$, this gives $N_2 = 6$ and when $r = 3$, it gives $N_3 = 17$.

We use this result to determine, among all isomorphism classes of hyperfields of order at most 4, precisely which ones are quotients of fields (finite or infinite). In addition to Theorem 1.1 and some routine case analysis, this requires a Ramsey-theoretic result proved independently by Bergelson–Shapiro and Turnwald [BS92, Tu94]. Our classification can be summarized as follows:

**Theorem 1.3.**

1. There are 2 isomorphism classes of hyperfields of order 2, the Krasner hyperfield and the finite field $\mathbb{F}_2$.
2. Every hyperfield of order 3 is a quotient of a field. More precisely, there are 5 isomorphism classes of hyperfields of order 3, all but one of which are isomorphic to quotients of finite fields. The hyperfield of signs is isomorphic to $\mathbb{R}/\mathbb{R}_+$ but not to any quotient of a finite field.
3. There are 8 isomorphism classes of hyperfields of order 4. Of these, 4 are quotients of finite fields, 1 is a quotient of an infinite field but not of any finite field, and the remaining 3 are not quotients of any field.

Content overview. In Section 2, we provide some background information on hyperfields. Theorem 1.1 will be proved in Section 3 and Theorem 1.3 will be proved in Section 4. We conclude in Section 5 with some open questions.

2. Hyperfields

**Definition 2.1.** A hyperoperation on a set $F$ is a binary map

$$\oplus: \quad F \times F \rightarrow \mathcal{P}(F)$$

to the power set of $F$ such that $a \oplus b$ is non-empty for all $a, b \in F$.

A hyperoperation is called commutative if $a \oplus b = b \oplus a$ for all $a, b \in F$, and associative if

$$\bigcup_{d \in b \oplus c} a \oplus d = \bigcup_{d \in a \oplus b} d \oplus c$$

for all $a, b, c \in F$.

**Definition 2.2.** A hypergroup is a set $G$ equipped with an associative hyperoperation $\oplus$ satisfying the following axioms:

1. There is an element $0 \in G$ such that $0 \oplus a = a \oplus 0 = \{a\}$. (identity element)
2. There is a unique element $-a$ in $G$ such that $0 \in a \oplus (-a)$. (inverses)
3. $a \in b \oplus c$ if and only if $-b \in (-a) \oplus c$. (reversibility)

A hypergroup is called commutative if the endowed hyperoperation is commutative.

**Definition 2.3.** A hyperfield is a set $\mathbb{H}$ equipped with a binary operation $\cdot$, a hyperoperation $\oplus$, and distinct elements $0, 1 \in \mathbb{H}$ satisfying the following axioms:

1. $(\mathbb{H}, \oplus, 0)$ is a commutative hypergroup.
(2) \((\mathbb{H}^x, \cdot, 1)\) is an abelian group.
(3) \(a \cdot 0 = 0 \cdot a = 0\) for all \(a \in \mathbb{H}\).
(4) \(a \cdot (b \boxplus c) = ab \boxplus ac\) for all \(a, b, c \in \mathbb{H}\), where \(a \cdot (b \boxplus c)\) is defined as \(\{ad \mid d \in b \boxplus c\}\).

It follows easily from the definitions that \((-1)^2 = 1\) in any hyperfield \(\mathbb{H}\).

Some important examples of hyperfields are as follows:

(1) Every field \(F\) is tautologically a hyperfield by defining \(a \boxplus b = \{a + b\}\).

(2) The Krasner hyperfield \(\mathbb{K} = \{0, 1\}\) is equipped with the usual multiplication and hyperaddition characterized by \(1 \boxplus 1 = \{0, 1\}\).

(3) The hyperfield of signs \(\mathbb{S} = \{0, 1, -1\}\) is equipped with the usual multiplication and hyperaddition characterized by the rules \(1 \boxplus 1 = \{1\}\), \(-1 \boxplus -1 = \{-1\}\) and \(1 \boxplus -1 = \{0, 1, -1\}\).

(4) The weak hyperfield of signs \(\mathbb{W} = \{0, 1, -1\}\) is equipped with the usual multiplication and hyperaddition characterized by the rules \(1 \boxplus 1 = -1 \boxplus -1 = \{1, -1\}\) and \(1 \boxplus -1 = \{0, 1, -1\}\).

Let \(F\) be a field and let \(G\) be a subgroup of \(F^\times\). The multiplicative monoid \(F/G = (F^\times/G) \cup \{0\}\) can be endowed with a natural hyperfield structure by setting

\[
[a] \boxplus [b] = \{ [c] \mid c = a' + b' \text{ for some } a' \in [a], b' \in [b] \}.
\]

We call hyperfields of this form quotient hyperfields. The four examples given above are all quotient hyperfields: indeed, we have \(\mathbb{K} = F/F^\times\) for any field \(F\) with more than two elements, \(\mathbb{S} = \mathbb{R}/\mathbb{R}_+\), and \(\mathbb{W} = \mathbb{F}_p/(\mathbb{F}_p^\times)^2\) for any prime number \(p \geq 7\) with \(p \equiv 3 \pmod{4}\).

**Definition 2.4.** Let \(\mathbb{H}_1\) and \(\mathbb{H}_2\) be hyperfields. A map \(\phi: \mathbb{H}_1 \to \mathbb{H}_2\) is called a hyperfield homomorphism if \(\phi(0) = 0, \phi(1) = 1, \phi(ab) = \phi(a)\phi(b), \text{ and } \phi(a \boxplus_1 b) \subset \phi(a) \boxplus_2 \phi(b)\) for all \(a, b \in \mathbb{H}_1\).

A homomorphism of hyperfields \(\phi: \mathbb{H}_1 \to \mathbb{H}_2\) is an isomorphism if there is an inverse homomorphism \(\psi: \mathbb{H}_2 \to \mathbb{H}_1\). One easily checks that a homomorphism of hyperfields is an isomorphism if and only if it is bijective.

3. **Proof of Theorem 1.1**

Our proof of Theorem 1.1 is based on the following well-known inequality from number theory:

**Theorem 3.1** (Davenport–Hasse). Let \(a, b,\) and \(c\) be nonzero elements of the finite field \(\mathbb{F}_q\), and let \(r\) be a positive integer with \(r \mid q - 1\). Then the number \(M(q)\) of projective solutions in \(\mathbb{P}^2(\mathbb{F}_q)\) to the homogeneous equation \(ax^r + by^r + cz^r = 0\) satisfies

\[
|M(q) - (q + 1)| \leq (r - 1)(r - 2)q^{1/2}.
\]

**Proof.** See, e.g., [Co07, Corollary 2.5.23] for an “elementary” proof using Jacobi sums derived from the work of Davenport and Hasse [DH35]. The Davenport–Hasse theorem is a special case of the more general result, proved by Weil, that if \(C/\mathbb{F}_q\) is a nonsingular
projective curve of genus $g$ and $C(\mathbb{F}_q)$ denotes the set of points of $C$ over $\mathbb{F}_q$ then $|C(\mathbb{F}_q)| - (q + 1) \leq 2gq^{1/2}$. \hfill \Box$

We now give the proof of Theorem 1.1.

**Proof of Theorem 1.1.** Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements, and let $g$ be a generator of the multiplicative group $\mathbb{F}_q^\times$. Then for $r | q - 1$, the unique subgroup $G^r_q$ of $\mathbb{F}_q^\times$ of index $r$ is of the form

$$\{g^r, g^{2r}, \ldots, g^{sr}\},$$

where $q = sr + 1$. Given $i, j, k \in \{1, 2, \ldots, r\}$, the following are equivalent:

1. $[g^k] \in [g^i] \boxplus [g^j]$ in $\mathbb{H}$.
2. There exists at least one solution $(x, y, z) \in (\mathbb{F}_q^\times)^3$ to the homogeneous polynomial equation

\[
\begin{align*}
g^i x^r + g^j y^r - g^k z^r &= 0. \\
\end{align*}
\]

For projective solutions to (1) with $x = 0$, we have

$$g^j y^r - g^k z^r = 0,$$

or equivalently,

$$(z/y)^r = g^{j-k}.$$

Therefore the number of such solutions is at most $r$, and thus the equation (1) has at most $3r$ projective solutions with some coordinate equal to zero.

For $q \geq r^4$, Theorem 3.1 implies that the number $N(q)$ of projective solutions in $\mathbb{F}_q$ to

$$g^i x^r + g^j y^r - g^k z^r = 0$$

with $x, y, z$ all nonzero satisfies

\[
\begin{align*}
N(q) &\geq M(q) - 3r \\
&\geq (q + 1) - (r - 1)(r - 2)q^{1/2} - 3r \\
&= \sqrt{q} - (r - 1)(r - 2) - 3r + 1 \\
&\geq r^2(3r - 2) - 3r + 1 \\
&> 0
\end{align*}
\]

for $r \geq 2$.

It follows that $[g^k] \in [g^i] \boxplus [g^j]$ for all $i, j, k \in \{1, 2, \ldots, r\}$, i.e., $\mathbb{H}^\times \subseteq [g^i] \boxplus [g^j]$ for every $i, j \in \{1, 2, \ldots, r\}$.

It remains to determine the set of $[g^i], [g^j]$ such that $0 \in [g^i] \boxplus [g^j]$. By the distributivity axiom 2.3(4), the hyperaddition table for $\mathbb{H}$ is determined by the values of $[g] \boxplus [g^i]$ for $i = 1, 2, \ldots, r$. Thus, by 2.2(2), the entire hyperaddition table for $\mathbb{H}$, and hence the isomorphism class of $\mathbb{H}$ itself, is determined by the unique integer $m \in \{1, 2, \ldots, r\}$ such that $0 \in [g] \boxplus [g^m]$.

We have two cases depending on the parity of $r$.

**Case 1:** $r$ is odd.
We claim that \( m = 1 \), i.e., \( 0 \in [g] \oplus [g] \).

**Case 1a:** \( p = 2 \). In this case, the inclusion \( 0 \in [g] \oplus [g] \) follows easily from the fact that \( x + x = 0 \) for each \( x \in \mathbb{F}_q \).

**Case 1b:** \( q = p^n \) is an odd prime power. In this case, \( g \) and \( g^{\frac{q-1}{2}}r+1 \) both belong to \([g]\) and

\[
g^1 + g^{\left(\frac{q-1}{2}\right)r+1} = g(1 + g^{\left(\frac{q-1}{2}\right)r}) = g(1 + (-1)^r) = 0.
\]

It follows that \( \mathbb{H} \) is isomorphic to the hyperfield \( \mathbb{H}_r \) whose hyperaddition is defined by \([x] \oplus [0] = [x]; [x] \oplus [x] = \mathbb{H}_r \) for \( [x] \neq [0] \); and \([x] \oplus [y] = \mathbb{H}_r^\times \) for distinct nonzero \([x]\) and \([y]\).

**Case 2:** \( r \) is even.

In this case, we claim that \( m = 1 \) if \( q \equiv 1 \pmod{2r} \) and \( m = \frac{q}{2} + 1 \) if \( q \equiv r + 1 \pmod{2r} \).

**Case 2a:** \( q \equiv 1 \pmod{2r} \).

Write \( q = 2lr + 1 \). Then for \( g \) and \( g^{lr+1} \) in \([g]\), we have

\[
g^1 + g^{lr+1} = g(1 + g^{lr}) = g(1 + g^{\frac{q-1}{2}}) = 0.
\]

Thus \( m = 1 \) and \( \mathbb{H} \) is isomorphic to the hyperfield \( \mathbb{H}_r \) defined above.

**Case 2b:** \( q \equiv r + 1 \pmod{2r} \).

Write \( q = (2l + 1)r + 1 \). Then for \( g \in [g] \) and \( g^{lr+\frac{r}{2}+1} \in [g^{\frac{r}{2}+1}] \), we have

\[
g^1 + g^{lr + \frac{r}{2} + 1} = g(1 + g^{lr + \frac{r}{2}}) = g(1 + g^{\frac{q-1}{2}}) = 0.
\]

Thus \( m = \frac{q}{2} + 1 \) and \( \mathbb{H} \) is isomorphic to the hyperfield \( \mathbb{H}_r' \) whose hyperaddition is defined by \([x] \oplus' [0] = [x]; [x] \oplus' [-x] = \mathbb{H}_r' \) for \( x \neq [0] \); and \([x] \oplus' [y] = \mathbb{H}_r'^\times \) otherwise.

Finally, note that \( \mathbb{H}_r \) and \( \mathbb{H}_r' \) are not isomorphic since if

\[
\phi : \mathbb{H}_r \rightarrow \mathbb{H}_r'
\]

was an isomorphism of hyperfields we would have

\[
\phi(\mathbb{H}_r) = \phi([1] \oplus [1]) = \phi([1]) \oplus' \phi([1]) = [1] \oplus' [1] = \mathbb{H}_r'^\times,
\]

a contradiction.

This concludes the proof of Theorem 1.1. \( \square \)
4. Proof of Theorem 1.3

In this section we prove Theorem 1.3 concerning the structure of hyperfields of order at most 4. In addition to Theorem 1.1, we will use the following result proved independently by Bergelson and Shapiro [BS92, Theorem 1.3] and Turnwald [Tu94, Theorem 1]:

**Theorem 4.1** (Turnwald). If $F$ is an infinite field and $G$ is a subgroup of $F^\times$ of finite index then $G - G = F$.

Here, as usual, $G - G$ denotes the set $\{x - y : x, y \in G\}$.

For the reader’s convenience, we present Turnwald’s elegant short argument below; it is an application of the Hales-Jewett theorem [HJ63] from Ramsey theory. (The argument of Bergelson–Shapiro uses a simpler variant of Ramsey’s theorem plus the amenability of finite groups.)

In order to state the Hales-Jewett theorem, define a subset $L_0 \subset \{1, \ldots, M\}$ to be a **combinatorial line** if there is a partition of $\{1, \ldots, N\}$ into disjoint subsets $J_0$ and $J_1$, with $J_1 \neq \emptyset$, and elements $k'_j \in \{0, \ldots, m\}$ for $j \in J_0$ such that

$$L = \{(k_1, \ldots, k_N) : k_j = k'_j \text{ for } j \in J_0 \text{ and } k_{j_1} = k_{j_2} \text{ for } j_1, j_2 \in J_1\}.$$  

The Hales-Jewett theorem asserts that for every $m, n \in \mathbb{N}$ there exists $N(m, n) \in \mathbb{N}$ such that if $S$ is a set, $N \geq N(m, n)$, and $f : \{0, \ldots, m\}^N \to S$ is a function taking on at most $n$ values, then $f$ must be constant on some combinatorial line.

**Proof.** (Proof of Theorem 4.1) Let $x_0 = 0$ and let $x_1, \ldots, x_r \in F$ be a set of (left) coset representatives for $G$ in $F^\times$. We claim that there exists $c \in F^\times$ such that $1 + cx_i \in G$ for all $i = 1, \ldots, r$. Given the claim, if we let $y_i = cx_i$ then $y_1, \ldots, y_r$ also form a set of coset representatives for $G$ and $1 + y_i \in G$ for all $i$. It follows that $y_i G \subseteq G - G$ for all $i$, and hence $G - G = F$ as desired.

To prove the claim, let $N = N(r, r + 1)$ be the bound given in the Hales-Jewett theorem. Since $F$ is infinite, there exist $c_1, \ldots, c_N \in F$ so that $\sum_{j \in J} c_j \neq 0$ for all non-empty subsets $J \subseteq \{1, \ldots, N\}$ (choose $c_k$ inductively so that $\sum_{j \in J} c_j \neq 0$ for all $J \subseteq \{1, \ldots, k\}$). Let $\mathbb{H} = F/G$, and define $f : \{0, \ldots, r\}^N \to \mathbb{H}$ by $f(k_1, \ldots, k_N) = [\sum_{j=1}^N c_j x_k]$. By the Hales-Jewett theorem, there is a partition of $\{1, \ldots, N\}$ into disjoint subsets $J_0$ and $J_1$, with $J_1 \neq \emptyset$, and elements $k'_j \in \{0, \ldots, r\}$ for $j \in J_0$ such that $f$ is constant on the corresponding combinatorial line $L$. Unwinding the definitions, this means that $[a + bx_k]$ is constant for all $0 \leq k \leq r$, where $a = \sum_{j \in J_0} c_j x_k'$ and $b = \sum_{j \in J_1} c_j$. Since $x_0 = 0$, this constant value is equal to $[a]$, and thus $aG = (a + bx_k)G$ for all $k = 1, \ldots, r$. Setting $c = a^{-1}b$ establishes the claim. (Note that $a \neq 0$ since $b \neq 0$ and $x_k \neq 0$ for $k \in \{1, \ldots, r\}$.) \(\square\)

**Remark 4.2.** The same proof applies verbatim if $F$ is replaced by an infinite division ring which is not necessarily commutative.

**Remark 4.3.** If $[F^\times : G]$ is odd, note that $-1 \in G$ since $[-1]^2 = [1]$ in the odd-order group $F^\times/G$, and hence $G - G = G + G$.

We are now ready to prove Theorem 1.3.
Proof of Theorem 1.3. We consider separately the cases where \(|\mathbb{H}|\) is equal to 2, 3, or 4.

**Case 1:** Hyperfields of order 2. It is clear by inspection that every hyperfield of order 2 is isomorphic to either the Krasner hyperfield \(\mathbb{K}\) or the field \(\mathbb{F}_2\) of two elements. Moreover, \(\mathbb{K}\) is isomorphic to \(F/F^\times\) for any field \(F\). This proves part (1) of Theorem 1.3.

**Case 2:** Hyperfields of order 3.

Let \(\mathbb{H}\) be a hyperfield with \(|\mathbb{H}| = 3\). The multiplicative group \(\mathbb{H}^\times\) must be cyclic of order 2, so we can write \(\mathbb{H} = \{0, 1, g\}\) with \(g^2 = 1\) and \(g \neq 1\). (We note that \(g\) might or might not be equal to \(-1\) in \(\mathbb{H}\).) A straightforward case analysis using the hyperfield axioms now shows that there are precisely 5 possible hyperaddition structures for \(\mathbb{H}\). Indeed, by the distributive law (Definition 2.3(4)) the hyperaddition table for \(\mathbb{H}\) is completely determined by \(1 \boxplus 1\) and \(1 \boxplus g\), and only the following 5 possibilities are compatible with the associativity of \(\boxplus\) and the reversibility axiom (Definition 2.2(3)):

1. \(1 \boxplus 1 = \{g\}\) and \(1 \boxplus g = \{0\}\). In this case, \(\mathbb{H} \cong \mathbb{F}_3\).
2. \(1 \boxplus 1 = \{0, g\}\) and \(1 \boxplus g = \{1, g\}\). In this case, \(\mathbb{H} \cong \mathbb{F}_5/G_2^2\).
3. \(1 \boxplus 1 = \{0, g^2\}\) and \(1 \boxplus g = \mathbb{H}^\times\). In this case, \(\mathbb{H} \cong \mathbb{H}_2 \cong \mathbb{F}_q/G_q^2\) for all prime powers \(q \geq 7\) and \(q \equiv 1\) (mod 4).
4. \(1 \boxplus 1 = \mathbb{H}^\times\) and \(1 \boxplus g = \mathbb{H}^\times\). In this case, \(\mathbb{H} \cong \mathbb{H}_4 \cong \mathbb{F}_q/G_q^2\) for all prime powers \(q \geq 7\) and \(q \equiv 3\) (mod 4).
5. \(1 \boxplus 1 = \{1\}\) and \(1 \boxplus g = \mathbb{H}\). In this case, \(\mathbb{H} \cong \mathbb{S} \cong \mathbb{R}/\mathbb{R}_+\).

It is straightforward to verify that none of these five hyperfields is isomorphic to any other one.

Moreover, \(\mathbb{S}\) is not isomorphic to a quotient of any finite field \(\mathbb{F}_q\) because otherwise there would be a homomorphism \(\mathbb{F}_q \rightarrow \mathbb{S}\) and hence, by [Ma06, Section 3], an ordering on \(\mathbb{F}_q\); however, it is well known that every ordered field has characteristic zero. (Indeed, if \(F\) were an ordered field of characteristic \(p > 0\) then we would have \(-1 = p - 1 = 1 + 1 + \cdots + 1\) \((p - 1\) times) \(> 0\), a contradiction.) Alternatively, using Remark 1.2, it suffices to check that \(\mathbb{F}_q/G_q^2 \neq \mathbb{S}\) for \(q \leq 5\), which is straightforward.

This proves part (2) of Theorem 1.3.

**Case 3:** Hyperfields of order 4.

Let \(\mathbb{H}\) be a hyperfield with \(|\mathbb{H}| = 4\). The multiplicative group \(\mathbb{H}^\times\) must be cyclic of order 3, so we can write \(\mathbb{H} = \{0, 1, g, g^2\}\) with \(g^3 = 1\). Note in this case that \(1 \neq -1\) in \(\mathbb{H}\), since \(\mathbb{H}^\times\) contains no element of order 2. A tedious, but still straightforward, case analysis using the hyperfield axioms now shows that there are precisely 8 possible hyperaddition structures for \(\mathbb{H}\):

1. \(1 \boxplus 1 = \{0\}\) and \(1 \boxplus g = \{g^2\}\). In this case, \(\mathbb{H} \cong \mathbb{F}_4\).
2. \(1 \boxplus 1 = \{0, g^2\}\) and \(1 \boxplus g = \{g, g^2\}\). In this case, \(\mathbb{H} \cong \mathbb{F}_7/G_3^2\).
3. \(1 \boxplus 1 = \{0, g^2\}\) and \(1 \boxplus g = \mathbb{H}^\times\). In this case, \(\mathbb{H} \cong \mathbb{F}_{13}/G_{13}^1 \cong \mathbb{F}_{16}/G_{16}^3\).
4. \(1 \boxplus 1 = \mathbb{H}\) and \(1 \boxplus g = \mathbb{H}^\times\). In this case, \(\mathbb{H} \cong \mathbb{F}_q/G_q^2\) for all prime powers \(q \geq 19\).
5. \(1 \boxplus 1 = \{0, g, g^2\}\) and \(1 \boxplus g = \{1, g^2\}\).
6. \(1 \boxplus 1 = \{0, g, g^2\}\) and \(1 \boxplus g = \{1, g\}\).
7. \(1 \boxplus 1 = \{0, 1, g\}\) and \(1 \boxplus g = \{1, g^2\}\).
(8) \(1 \oplus 1 = \mathbb{H}\) and \(1 \oplus g = \{1, g\}\).

It is straightforward to verify that none of these eight hyperfields is isomorphic to any other one.

To see that none of the hyperfields in (5)-(8) is a quotient of a finite field \(\mathbb{F}_q\), it suffices by Remark 1.2 to check that none of the hyperfields in (5)-(8) is isomorphic to \(\mathbb{F}_q/G_q^3\) for some \(q \leq 16\). We omit the details of this straightforward computation.

The hyperfield \(\mathbb{H}\) in (8) can, however, be realized as the quotient of an infinite field. For example (cf. [LS89, Proposition 6]), choose a prime number \(p\), let \(\text{ord}_p\) denote the \(p\)-adic valuation on \(\mathbb{Q}\), and let \(G\) be the index 3 subgroup of \(\mathbb{Q}^\times\) consisting of all rational numbers \(x = a/b\) such that \(\text{ord}_p(x)\) is a multiple of 3. It is straightforward to check, using the ultrametric inequality, that \(\mathbb{H} \cong \mathbb{Q}/G\).

On the other hand, by Theorem 4.1 and Remark 4.3, none of the hyperfields in (5)-(7) can be the quotient of an infinite field since \(G + G = G - G = F\) implies that \(1 \oplus 1 = \mathbb{H}\), but in each of (5)–(7) we have \(1 \oplus 1 \neq \mathbb{H}\).

This proves part (3) of Theorem 1.3. \(\square\)

**Remark 4.4.** Theorem 4.1 also yields the following generalization of Massouros’s example [Ma85] mentioned in Section 1: if \(\mathbb{H}\) is a hyperfield such that \(\mathbb{H}^\times\) is not cyclic and \(1 \oplus (-1) \neq \mathbb{H}\), then \(\mathbb{H}\) is not a quotient hyperfield. Indeed, the former condition implies that \(\mathbb{H}\) is not a quotient of a finite field and the latter implies that \(\mathbb{H}\) is not a quotient of an infinite field.

5. Some open questions

We conclude with a few open questions.

1. What is the true order of growth of \(N_r\) in Theorem 1.1? In other words, how small can we take \(N_r\) so that all hyperfields of the form \(\mathbb{F}_q/G_q^r\) with \(q \geq N_r\) and \(q \equiv 1\) (mod \(r\)) are isomorphic to either \(\mathbb{H}_r\) or \(\mathbb{H}'_r\)? For \(r = 2\) and \(r = 3\) the upper bound for \(N_r\) given by Remark 1.2 is sharp; what happens in general? (Taking \(\mathbb{H} = \mathbb{F}/\mathbb{F}_p^\times\) with \(p = r - 1\) shows that \(N_r > (r - 1)^2\) whenever \(r - 1\) is prime, but this is quite far from the upper bound furnished by Remark 1.2.)

2. Let \(H_r\) be the number of isomorphism classes of hyperfields of order \(r + 1\), and let \(Q_r\) be the number of isomorphism classes of quotient hyperfields of order \(r + 1\). How do the relative growth rates of \(H_r\) and \(Q_r\) compare? We conjecture, based on the considerations in this paper, that \(Q_r/H_r\) tends to zero as \(r\) tends to infinity. (If true, this would mean colloquially speaking that “almost all” hyperfields are not quotients of fields.)

3. Is there an algorithm to determine whether or not a given finite hyperfield is a quotient of some infinite field?

References

[BS92] V. Bergelson and D. Shapiro. Multiplicative subgroups of finite index in a ring. *Proceedings of the Amer. Math. Soc.*, 116(4):885-896, 1992.

[Co07] H. Cohen. *Number Theory. Volume I: Tools and Diophantine Equations*. Volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.
[DH35] H. Davenport and H. Hasse. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *J. Reine Angew. Math.*, 172:151-182, 1935.

[HJ63] A. Hales and R. Jewett. Regularity and positional games. *Transactions of the Amer. Math. Soc.*, 106(2):222-229, 1963.

[LS89] D. Leep and D. Shapiro. Multiplicative subgroups of index three in a field. *Proceedings of the Amer. Math. Soc.*, 105(4):802-807, 1989.

[Kr83] M. Krasner. A class of hyperrings and hyperfields. *Intern. J. Math. Math. Sci.*, 6(2):307-312, 1983.

[Ma06] M. Marshall. Real reduced multirings and multifields. *J. Pure Appl. Algebra*, 205(2):452-468, 2006.

[Ma85] Ch. G. Massouros. Methods of constructing hyperfields. *Intern. J. Math. Math. Sci.*, 8(4):725-728, 1985.

[Tu94] G. Turnwald. Multiplicative subgroups of finite index in a division ring. *Proceedings of the Amer. Math. Soc.*, 120(2):377-381, 1994.

*E-mail address*: mbaker@math.gatech.edu

**SCHOOL OF MATHEMATICS, GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, USA**

*E-mail address*: tongjin@gatech.edu

**TAISHAN COLLEGE, SHANDONG UNIVERSITY, JINAN, CHINA**