Powerful sets: a generalisation of binary matroids

Graham E. Farr*
Faculty of Information Technology
Monash University
Clayton, Victoria 3800
Australia
Graham.Farr@monash.edu

Andrew Y.Z. Wang†
School of Mathematical Sciences
University of Electronic Science and Technology of China
Chengdu 611731
P.R. China
yzwang@uestc.edu.cn

Submitted: Jan 24, 2018; Accepted: Aug 7, 2018; Published: Sep 7, 2018

Abstract

A set $S \subseteq \{0,1\}^E$ of binary vectors, with positions indexed by E, is said to be a *powerful code* if, for all $X \subseteq E$, the number of vectors in S that are zero in the positions indexed by X is a power of 2. By treating binary vectors as characteristic vectors of subsets of E, we say that a set $S \subseteq 2^E$ of subsets of E is a *powerful set* if the set of characteristic vectors of sets in S is a powerful code. Powerful sets (codes) include cocircuit spaces of binary matroids (equivalently, linear codes over $\mathbb{F}_2$), but much more besides. Our motivation is that, to each powerful set, there is an associated nonnegative-integer-valued rank function (by a construction of Farr), although it does not in general satisfy all the matroid rank axioms.

In this paper we investigate the combinatorial properties of powerful sets. We prove fundamental results on special elements (loops, coloops, frames, near-frames, and stars), their associated types of single-element extensions, various ways of combining powerful sets to get new ones, and constructions of nonlinear powerful sets. We show that every powerful set is determined by its clutter of minimal nonzero members. Finally, we show that the number of powerful sets is doubly exponential, and hence that almost all powerful sets are nonlinear.

Mathematics Subject Classifications: 05B35, 05B99, 94B60, 94B05

*This work was presented at the 40th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing (40ACCMCC), University of Newcastle, Australia, Dec. 2016.

†Most of the work of this paper was done while Wang was a Visiting Scholar in the Faculty of I.T., Monash University, Oct. 2015 – Oct. 2016, funded by the China Scholarship Council (CSC).

1 Introduction

Let E be a finite set, called the *ground set*, and let $S \subseteq \{0,1\}^E$ be a set of binary vectors, with positions indexed by E. A set $X \subseteq E$ of positions has the *power-of-2 property (for S)* if the number of vectors in S that are zero on X (i.e., in the positions indexed by X) is a power of 2. We say S is a *powerful set*, or a *powerful code*, if every $X \subseteq E$ has the power-of-2 property for S. By treating binary vectors as characteristic vectors of subsets of E, we also say that a set $S \subseteq 2^E$ of subsets of E is a *powerful set* if the set of characteristic vectors of sets in S is a powerful set. We move freely between subsets X of E and their characteristic vectors $\mathbf{x}$. We prefer powerful *set* terminology, but sometimes use powerful *code* terminology when commenting on connections with coding theory.

Unless stated otherwise, we use the ground set $E = [n] := \{1, 2, \ldots, n\}$. We view S as a subset of the n-dimensional linear space $\mathbb{F}_2^n$, over the finite field $\mathbb{F}_2$ consisting of all 01-vectors of length n.

The *order* of a powerful set S is the size of its ground set, or equivalently, the length of its vectors (when S is viewed as a code). The *size* of S is the cardinality of S. The power-of-2 property for $X = E$ implies that the zero vector must be in S. With $X = \varnothing$, we conclude that the size of S is also a power of 2. The *dimension* of S, written $\dim S$, is the nonnegative integer d such that the size of S is 2^d.

Two powerful sets S_1 and S_2 are said to be *isomorphic*, written $S_1 \cong S_2$, if there is a bijection between their ground sets which induces a bijection between S_1 and S_2.

If S is a finite-dimensional linear space over $\mathbb{F}_2$, then the vectors of S that are 0 on X form a subspace of S, thus the number of such vectors is a power of 2. Hence such a linear space is always a powerful set. From now on, we say a powerful set S is *linear* if it is a linear space, otherwise it is *nonlinear*. Up to isomorphism, there is a unique smallest nonlinear powerful set, namely

$$S = \{000, 011, 101, 111\}.$$

Later we will see that almost all powerful sets are nonlinear.

For the sake of convenience, we often write a set $S \subseteq \mathbb{F}_2^n$ in the form of a matrix whose rows are the elements of S. For example, we can identify the above smallest nonlinear powerful set S with the matrix

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

We emphasise that, when S is linear, this is not just a generator matrix for S; its rows list *all* members of S.

Our remarks above show that powerful sets generalise binary matroids, or equivalently, binary linear codes. Every binary matroid has a rank function $\rho : 2^E \to \mathbb{N} \cup \{0\}$, defined on subsets of its ground set E, that satisfies the matroid rank axioms. Our original motivation for studying powerful sets was that they, too, have a nonnegative-integer-

valued "rank-like" function. We elaborate on this now, before setting the scene for the rest of this paper.

Let $f : 2^E \to \{0,1\}$ be the indicator function of a binary code $S \subseteq \mathbb{F}_2^E$, defined for any $X \subseteq E$ by $f(X) = 1$ or 0 according as the characteristic vector of X does, or does not, belong to S. The *rank transform* Q, introduced in [2] (see also the exposition in [4, §3.6] and a closely related construction due to Kung [5]), associates to any such f the function Qf defined on subsets of E by

$$Qf(X) = \log_2 \left(\frac{\sum_{Y \subseteq E} f(Y)}{\sum_{Y \subseteq E \setminus X} f(Y)} \right). \tag{1.1}$$

Observe that, when $Qf(X)$ is defined, it must be nonnegative. (This follows from the fact that f itself is nonnegative-valued.) When it is defined, we call $Qf(X)$ the *rank* of X, but bear in mind that this is a loosening of that term since Qf may not satisfy the matroid rank axioms. For the special case when S is linear, Qf gives the usual rank function for the binary matroid. If S is nonlinear, then Qf may take irrational values or be undefined for some arguments. For $Qf(X)$ to be defined for all $X \subseteq E$, it is necessary and sufficient that $f(\varnothing) = 1$. In particular, $Qf(X)$ is always defined if S is a powerful set, since in that case $\varnothing \in S$ so $f(\varnothing) = 1$. For Qf to be integer valued, it is necessary and sufficient that S be a powerful set.

If $f(\varnothing) = 1$ then (using the nonnegativity of f) $Qf(\varnothing) = 0$, and $Qf(X) \leqslant Qf(Y)$ whenever $X \subseteq Y$. These are among the properties that hold for any matroid rank function. But Qf need not satisfy other matroid rank properties. It is possible that $Qf(X) > |X|$ (see §3), and *submodularity* — $\rho(X \cap Y) + \rho(X \cup Y) \leqslant \rho(X) + \rho(Y)$ for all X, Y — need not hold for $\rho = Qf$ (consider, e.g., $S = \{00, 01, 10\}$ [2, Example 2.2], or see below for a powerful set example).

Not only does f determine Qf, but when $f(\varnothing) = 1$ the reverse holds too: Qf determines f. See [2] for details of the *inverse rank transform* $Q^\dagger$, which satisfies $Q^\dagger Qf \equiv f$ when $f(\varnothing) = 1$.

Given that the functions Qf extend rank functions, it is natural to investigate what happens when they are used in place of rank functions. This was done in [2, 3], where a theory of Tutte-Whitney polynomials is developed for arbitrary functions $f : 2^E \to \mathbb{C}$ (called *binary functions*). There, Qf is used in place of a matroid rank function to generalise the rank generating function of Whitney [10] to arbitrary binary functions. A surprising amount of Tutte-Whitney polynomial theory extends to these objects, including duality, deletion-contraction relations, and interesting partial evaluations. But the "polynomials" themselves often have nonintegral exponents. It is therefore natural to focus on cases where the *polynomials* are just that, which means that Qf is integer valued. If, in addition, we ask that f be $\{0,1\}$-valued, so that it is indeed an indicator function and can be taken to represent a subset of 2^E, then we are led to the study of powerful sets.

If S is a powerful set, we write f_S for its indicator function, and ρ_S for its rank function, $\rho_S := Qf_S$. Applying (1.1), we have, for any $X \subseteq E$,

$$\rho_S(X) = \dim S - \log_2 |\{\mathbf{y} \in S \mid y_i = 0 \ \forall i \in X\}|. \tag{1.2}$$

Observe that $\rho_S(E) = \dim S$ and $|S| = 2^{\rho_S(E)}$. Using the inverse rank transform of [2], the rank function ρ_S determines f_S and hence S.

We will see in §3, when we meet frames, that in powerful sets it is possible to have $\rho_S(X) > |X|$. Furthermore, in §5 we will meet cases where submodularity does not hold. These two failures of matroid axioms can be arbitrarily severe, so powerful sets can be very different to matroids (or polymatroids, which still require submodularity).

The definition of powerful codes is somewhat reminiscent of almost affine codes, introduced in [6], although they are different in nature. A q-ary code S with index set E is *almost affine* if for all $X \subseteq E$ the cardinality of the code $S_{E\setminus X} := \{(a_i)_{i\in E\setminus X} \mid (a_i)_{i\in E} \in S\}$ is a power of q. The construction of $S_{E\setminus X}$ from S is called *puncturing* with respect to X, or *projection* onto $E\setminus X$. We simply discard all coordinates with positions in X, thereby shortening the vectors to length $|E \setminus X|$. This contrasts with powerful sets, where we do not remove any coordinates, but simply require that the coordinates indexed by X are zero. When $q = 2$, a binary code containing the zero vector is almost affine if and only if it is linear [6], so binary almost affine codes give us nothing new, and correspond to binary matroids. See [6, 9] for further information about almost affine codes and their connections with matroid theory.

Powerful codes are also reminiscent of ideal secret sharing schemes: see [1, Proposition 1]. This is another manifestation of their superficial resemblance to almost affine codes, since connected ideal perfect secret sharing schemes are almost affine codes [1, Proposition 1] (see [6, §3.1]), and for the binary case all secret sharing schemes are perfect and ideal.

In this paper we lay the foundations of the theory of powerful sets. We first (in §2) extend the contraction operation, for binary matroids, to powerful sets. Then, in §3, we consider five types of special elements: loops, coloops, frames, near-frames, and stars. Of these, only loops and coloops occur in binary matroids. Each of the five has an associated type of single-element extension operation, and we also generalise parallel extensions from binary matroids to powerful sets. In §4, we present a construction for some nonlinear powerful sets, analogous to generating linear spaces from sets of vectors but using positionwise maximum instead of positionwise addition in $\mathbb{F}_2$ (i.e., positionwise OR instead of positionwise XOR). In §5 we give three ways of combining powerful sets to form new powerful sets. Two of these have no real analogue for linear spaces. Then in §6 we show that every powerful set is determined by its clutter of minimal nonzero members, by giving an algorithm to construct it from that clutter. Finally, we consider enumeration of powerful sets in §7. We report the numbers of powerful sets (and, in particular, the numbers of nonlinear powerful sets) of each order $\leqslant 6$. The trend in this data is that nonlinear powerful sets quickly dominate, and we confirm this trend mathematically. We show that the number of loopless frameless nonlinear powerful sets of order $n \geqslant 5$ is doubly exponential — specifically, at least $2^{2^{(n-7)/3}}$ — from which it follows that, asymptotically, almost all powerful sets are nonlinear.

Some notation: if $\mathbf{x}$ and $\mathbf{y}$ are vectors indexed by $[n]$ and $[m]$ respectively, then their *concatenation* $\mathbf{xy}$ denotes the vector indexed by $[n + m]$ whose first n elements are $\mathbf{x}$ and whose last m elements are $\mathbf{y}$. If, in addition, $b \in \{0, 1\}$, then $\mathbf{x}b$ denotes the vector indexed by $[n + 1]$ whose first n elements are $\mathbf{x}$ and whose last element is b.

2 Reductions

Let $S \subseteq 2^E$ and $e \in E$. Put

$$S/e := \{X \subseteq E\backslash\{e\} \mid X \in S\}.$$

We say that S/e is formed from S by *contraction* of e. In terms of matrix representation, we remove column e and also remove all rows that have a 1 in the position indexed by e.

For example, consider the (nonlinear) powerful set $S = \{000, 011, 110, 111\}$, with the usual ground set $\{1, 2, 3\}$. Then

$$\begin{array}{rcll} S/1 & = & \{00, 11\}, & \text{with ground set } \{2, 3\}; \\ S/2 & = & \{00\}, & \text{with ground set } \{1, 3\}; \\ S/3 & = & \{00, 11\}, & \text{with ground set } \{1, 2\}. \end{array}$$

So $S/1 \cong S/3$.

Theorem 1. *(a) If S is powerful then S/e is powerful.*
(b) If S is linear then S/e is linear. (See, e.g., [7, Theorem 9.3.1].)

The converses are not true, since (for example) adding a new all-0 column, indexed by e, to S/e (using the matrix representation viewpoint), then adding a row that is all-0 across $E\backslash\{e\}$ but has 1 in position e, does not in general give another powerful set (let alone a linear one).

The rank of S/e is given by $\rho_{S/e}(X) = \rho_S(X \cup \{e\}) - \rho_S(\{e\})$; see [2, §4].

Another way of reducing a powerful set by a single element is to simply delete the column indexed by e, without deleting any rows. We call this *deletion*, since it generalises deletion in binary matroids, and denote the subset of $2^{E\backslash\{e\}}$ so formed by $S\backslash e$. But, if it is applied to a nonlinear powerful set, it may leave duplicate rows in the reduced matrix, giving a powerful multiset but not necessarily a powerful set. The operation of *puncturing* with respect to e consists of deletion of e followed by removal of one member of each pair of identical rows. This ensures that we obtain a set rather than a multiset, and it yields a linear powerful set if S is linear (see, e.g., [7]), but it does not necessarily produce a powerful set if S is nonlinear. Note also that the addition of a new column to a powerful set (i.e., the reverse of puncturing) does not necessarily give a powerful set.

3 Extensions and special elements

We now look at several ways to extend a powerful set by a single element. A special role is played by five types of special elements. The proofs are straightforward and most are omitted.

An element $e \in E$ that belongs to no set in S (equivalently, it indexes a zero column in the matrix representation) is a *loop*, and has rank 0. The operation of adding a zero column to $T \subseteq \mathbb{F}_2^n$ is called *loop extension*, and the resulting subset of $\mathbb{F}_2^{n+1}$ is denoted by $T + \circ$. Observe that, if e is a loop of S, then $S\backslash e = S/e$.

Theorem 2. *If $e \in E$ is a loop of S and S/e is powerful then S is powerful.*

Suppose that, writing e as the last column and reordering rows if necessary, $S \subseteq \mathbb{F}_2^n$ has a matrix of the form

$$\begin{pmatrix} T & \mathbf{0} \\ T & \mathbf{1} \end{pmatrix},$$

where $T \subseteq \mathbb{F}_2^{n-1}$, and $\mathbf{0}$ and $\mathbf{1}$ are column vectors whose length equals the size of T. Then e is a *coloop* of S, and has rank 1. The operation of forming S from T in this way is called *coloop extension*. We write $S = T + \circ^*$.

Theorem 3. *If $e \in E$ is a coloop of S and S/e is powerful then S is powerful.*

Proof. For any $X \subseteq E$, if $e \notin X$, then the number of vectors of S that are 0 on X is twice the number of vectors of S/e that are 0 on X, thus being a power of 2.

If $e \in X$, then the number of vectors of S that are 0 on X is the same as the number of vectors of S/e that are 0 on $X\backslash\{e\}$, which is also a power of 2. □

Proposition 4. *If $e \in E$ is a coloop of S and S/e is linear then S is linear.*

Proof. For convenience, we write e as the last column in the matrix representation of S. Let $\mathbf{u}i$ and $\mathbf{v}j$ be any two vectors of S where $\mathbf{u}, \mathbf{v} \in S/e$ and $i, j \in \{0, 1\}$. It follows from the linearity of S/e that $\mathbf{w} = \mathbf{u} + \mathbf{v} \in S/e$. Thus we have $\mathbf{w}0 \in S$ and $\mathbf{w}1 \in S$. Since $i + j \in \{0, 1\}$, we can conclude that

$$\mathbf{u}i + \mathbf{v}j = \mathbf{w}(i + j) \in S.$$

Thus S is linear. □

Remark. For a powerful set S, the zero row vector $\mathbf{0}$ belongs to S, thus $\mathbf{0}1 \in S + \circ^*$. Therefore, a coloop extension of a powerful set must have a vector of weight 1.

Conjecture 5. If T is a powerful set with at least one vector of weight 1, then T is a coloop extension of some powerful set S.

Remark. The conjecture is true for the linear case, since a singleton member of the cocircuit space of a binary matroid must be a coloop.

Let S be a powerful set, again with e indexing the last column in its matrix, and now with matrix of the form

$$\begin{pmatrix} \mathbf{0} & 0 \\ T\backslash\{\mathbf{0}\} & \mathbf{1} \end{pmatrix},$$

where T is a powerful set, $\mathbf{0}$ is a row vector, and $\mathbf{1}$ is a column vector. Note that $S\backslash e = T$. Then e is a *frame* of S (using terminology for an analogous concept in [8]), and adjoining e to T is called *framing* T by e. A frame e has rank equal to $\dim S$. If $\dim S \geqslant 2$ then $X = \{e\}$ satisfies $\rho_S(X) > |X|$, in contrast to matroid rank functions. (In fact, such cases give the greatest possible differences $\rho_S(X) - |X|$ and ratios $\rho_S(S)/|X|$, showing that these can be arbitrarily large for powerful sets.) We write $S = T + \square$.

Theorem 6. *Let $S \subseteq \mathbb{F}_2^E$ have a frame $e \in E$. Then $S\backslash e$ is powerful if and only if S is powerful.*

A powerful set can also be enlarged by an element that is almost, but not quite, a frame.

Suppose $S \subseteq \mathbb{F}_2^n$ and $\mathbf{v} \in S$ is a nonzero vector. The set $S + \square\backslash\mathbf{v}$ is formed by adding a new coordinate 0 to the zero vector $\mathbf{0}$ and $\mathbf{v}$, and a new coordinate 1 to the remaining vectors of S. The new element is called a *near-frame* and has rank $\dim S - 1$.

Theorem 7. *If S is powerful then $S + \square\backslash\mathbf{v}$ is powerful.*

If $T \subseteq \mathbb{F}_2^n$, define $T + \star \subseteq \mathbb{F}_2^{n+1}$ by

$$T + \star = \{\mathbf{v}0 \,|\, \mathbf{v} \in T\} \cup \{\mathbf{v}1 \,|\, \mathbf{v} \notin T\}.$$

We can represent $S = T + \star$ by the following matrix

$$S = \left(\begin{array}{c|c} & 0 \\ T & \vdots \\ & 0 \\ \hline & 1 \\ \overline{T} & \vdots \\ & 1 \end{array}\right).$$

We call the new element a *star*. If T is powerful then $T + \star$ has rank $n - \dim T$.

Theorem 8. *$T \subseteq \mathbb{F}_2^n$ is powerful if and only if $T + \star$ is powerful.*

Proof. Let $\overline{T}$ be the set $\mathbb{F}_2^n\backslash T$. For any $X \subseteq [n+1]$, if $n+1$ is not in X, then the number of rows that are 0 on X must be a power of 2. This is because the submatrix consisting of the first n columns is the linear space $\mathbb{F}_2^n$. If $n + 1 \in X$, we only need to consider the submatrix

$$S_T = \left(\begin{array}{c|c} & 0 \\ T & \vdots \\ & 0 \end{array}\right).$$

The rows of S_T that are 0 on $X\backslash\{n+1\}$ are precisely those that are 0 on X. So the number of such rows is a power of 2 if and only if T is a powerful set. Therefore S is powerful if and only if T is powerful. □

Conjecture 9. Suppose that S is a subset of $\mathbb{F}_2^n$ with 2^{n-1} elements, where $n \geqslant 2$. If S is a powerful set, then we can find a coordinate such that deleting this coordinate from all the elements of S yields the set $\mathbb{F}_2^{n-1}$, i.e., all the new vectors are distinguishable.

Remark. Conjecture 9 holds if S is linear, since in that case we have a binary matroid of rank $n-1$ on n elements, which must have a circuit, and deleting any element e in the

circuit gives a binary matroid $S\backslash e$ of rank $n-1$ on $n-1$ elements, whose cocircuit space is all of $\mathbb{F}_2^{n-1}$. For the nonlinear case, Conjecture 9 holds for $n \leqslant 6$.

REMARK. If we do not require that the size of S is 2^{n-1}, Conjecture 9 fails to hold. For example, let

$$S = \{00000, 00111, 01011, 01111, 10101, 10111, 11010, 11011\}.$$

It is easy to check that S is a powerful set, but deleting any one coordinate will always yield two indistinguishable vectors of length 4.

REMARK. If a powerful set S satisfies Conjecture 9, it can always be constructed as $T + \star$ from a smaller powerful set T. Suppose that deleting the last bit of each vector in S gives all possible vectors of $\mathbb{F}_2^{n-1}$. Collecting those vectors of S whose last bit is 0 and removing the last bit from each such vector yields the desired smaller powerful set.

If S is a powerful set and $e \in E$, then the *parallel extension* of S, denoted by $S^{\shortparallel e}$, is formed by duplicating the column indexed by e in the matrix representation of S.

Theorem 10. *Let $S \subseteq 2^E$ and $e \in E$. Then S is powerful if and only if its parallel extension $S^{\shortparallel e}$ is powerful.*

From binary matroid theory, we have

Proposition 11. *Let S be a powerful set, then $S^{\shortparallel e}$ is linear if and only if S is linear.*

4 Position-wise max construction

Given any $S \subseteq \mathbb{F}_2^n$, elementary linear algebra gives us the linear powerful set $\langle S \rangle$ consisting of all binary linear combinations of vectors in S. In this section we give another way to generate larger sets from S, using a positionwise operation, which in this case will often give us nonlinear powerful sets.

A *permutation matrix* is a square binary matrix that has exactly one entry of 1 in each row and each column, and 0s elsewhere.

Given any $S \subseteq \mathbb{F}_2^n$, we consider its matrix representation. If the matrix representation of S contains a submatrix which is a permutation matrix of order $|S|$, then we say that S is *permutative*.

REMARK. It is clear that a permutative set cannot contain the zero vector.

Define the *disjunction* $\mathbf{u} \vee \mathbf{v}$ of two vectors $\mathbf{u} = (u_i)_{i=1}^n$ and $\mathbf{v} = (v_i)_{i=1}^n$ in $\mathbb{F}_2^n$ by $\mathbf{u} \vee \mathbf{v} = (\max\{u_i, v_i\})_{i=1}^n$.

Suppose $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m\} \subseteq \mathbb{F}_2^n$, define the *disjunctive closure* of S to be the set

$$\langle S \rangle_\vee = \{a_1\mathbf{u}_1 \vee a_2\mathbf{u}_2 \vee \cdots \vee a_m\mathbf{u}_m \,|\, a_i \in \mathbb{F}_2, 1 \leqslant i \leqslant m\},$$

where $a_i\mathbf{u}_i = \mathbf{u}_i$ if $a_i = 1$, and $\mathbf{0}$ otherwise. Note that the zero vector always belongs to $\langle S \rangle_\vee$.

Theorem 12. *If $m \leqslant n$ and $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m\} \subseteq \mathbb{F}_2^n$ is a permutative set, then $\langle S \rangle_\vee$ is a powerful set of size 2^m.*

Proof. Since we are not concerned with order on S or its ground set, we can assume that, in the matrix representation

$$S = \begin{pmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \\ \vdots \\ \mathbf{u}_m \end{pmatrix},$$

the first m columns form the identity matrix I_m.

We first prove that any vector in $\langle S\rangle_\vee$ has a unique expression as $a_1\mathbf{u}_1 \vee a_2\mathbf{u}_2 \vee \cdots \vee a_m\mathbf{u}_m$, which shows that the size of $\langle S\rangle_\vee$ is 2^m. Given a vector $\mathbf{v} = v_1v_2\cdots v_n \in \langle S\rangle_\vee$, we claim that

$$\mathbf{v} = v_1\mathbf{u}_1 \vee v_2\mathbf{u}_2 \vee \cdots \vee v_m\mathbf{u}_m.$$

That is to say, $\mathbf{v}$ is completely determined by its first m components. For $1 \leqslant i \leqslant m$, $\mathbf{u}_i$ is the only vector in S whose ith component is 1. So if $v_i = 1$, the coefficient of $\mathbf{u}_i$ must be 1 otherwise the ith component of $\mathbf{v}$ will be 0. Similarly, if $v_i = 0$, the coefficient of $\mathbf{u}_i$ is 0.

Next we show that $\langle S\rangle_\vee$ is a powerful set. Given $X \subset [n]$, let $\mathbf{u}_{1,X}, \mathbf{u}_{2,X}, \ldots, \mathbf{u}_{r,X} \in S$ be all vectors that are 0 on X. Then we claim that

$$\langle S\rangle_{\vee,X} := \{a_1\mathbf{u}_{1,X} \vee a_2\mathbf{u}_{2,X} \vee \cdots \vee a_r\mathbf{u}_{r,X} \,|\, a_i \in \mathbb{F}_2, 1 \leqslant i \leqslant r\}$$

contains all the vectors of $\langle S\rangle_\vee$ that are 0 on X. It is clear that any vector $\mathbf{w} \in \langle S\rangle_{\vee,X}$ is 0 on X. On the other hand, if $\mathbf{w} \in \langle S\rangle_\vee$ is 0 on X, then in the unique expression

$$\mathbf{w} = w_1\mathbf{u}_1 \vee w_2\mathbf{u}_2 \vee \cdots \vee w_m\mathbf{u}_m,$$

the coefficient of every $\mathbf{u}_i$ which is nonzero in some position in X must be zero, otherwise $\mathbf{w}$ has a nonzero entry in some position in X. Hence, the claim holds. In addition, any two vectors of $\langle S\rangle_{\vee,X}$ are different, thus the size of $\langle S\rangle_{\vee,X}$ is 2^r, a power of 2. If $X = [n]$, the zero vector is the only vector in $\langle S\rangle_\vee$ with all zero coordinates. Therefore, $\langle S\rangle_\vee$ is a powerful set. □

Example 13. Let $S = \{00011, 01100, 10101\} \subseteq \mathbb{F}_2^5$. Then the 1st, 2nd and 4th columns of

$$S = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

comprise a permutation matrix of order 3, thus S is permutative. We have

$$\langle S\rangle_\vee = \{00000, 00011, 01100, 10101, 01111, 10111, 11101, 11111\}.$$

It is straightforward to check that $\langle S\rangle_\vee$ is a powerful set.

If S is not permutative, then $\langle S\rangle_\vee$ is not necessarily powerful. For example, let $S = \{0111, 1011, 1101\}$, whose matrix representation has no unit vector columns so S is certainly not permutative. Then $\langle S\rangle_\vee = \{0000, 0111, 1011, 1101, 1111\}$, which has size 5, so is not powerful.

5 Combining two powerful sets

Basic set operations do not necessarily preserve the powerful property. The complement of a powerful set is never powerful (since it does not contain the zero vector), and the union and intersection of powerful sets are not necessarily powerful. (For example, take the linear powerful set $\{000, 011, 101, 110\}$ and our smallest nonlinear powerful set $\{000, 011, 101, 111\}$.)

We now present three ways to combine two powerful sets which give another powerful set (always, or under mild conditions). Only the first corresponds to a binary matroid operation.

Let $Q \subseteq \mathbb{F}_2^m$ and $R \subseteq \mathbb{F}_2^n$. The *direct sum* of Q and R is defined by

$$Q \oplus R = \{\mathbf{uv} \,|\, \mathbf{u} \in Q, \mathbf{v} \in R\}.$$

Theorem 14. *$Q \oplus R$ is powerful if and only if Q and R are powerful.*

Proof. If $X \subseteq [m]$ and $Y \subseteq \{m+1, \ldots, m+n\}$, then the number of vectors of $Q \oplus R$ that are zero on $X \cup Y$ is the number of vectors of Q that are zero on X times the number of vectors of R that are zero on Y. The result follows, paying particular attention to the case $X = \varnothing$ and the case $Y = \varnothing$. □

Elementary linear algebra gives

Proposition 15. *The direct sum $Q \oplus R$ is linear if and only if Q and R are both linear.*

The direct sum generalises the direct sum of binary matroids and is a special case of the product of disjoint binary functions [2, p. 276].

We now come to our second way of combining powerful sets.

Write $\mathbf{0}_k$ and $\mathbf{1}_k$ for the row vector of k 0s and k 1s, respectively.

Let $Q \subseteq \mathbb{F}_2^m$ and $R \subseteq \mathbb{F}_2^n$ be powerful sets. Define the set $Q\#R \subseteq \mathbb{F}_2^{m+n}$ as follows

$$Q\#R = \{\mathbf{0}_{m+n}\} \cup \{\mathbf{u}\mathbf{1}_n \,|\, \mathbf{u} \in Q \backslash \{\mathbf{0}_m\}\} \cup \{\mathbf{1}_m\mathbf{v} \,|\, \mathbf{v} \in R \backslash \{\mathbf{0}_n\}\} \cup \{\mathbf{1}_{m+n}\}.$$

The construction of $Q\#R$ can be depicted as

$$\left(\begin{array}{c|c} \mathbf{0}_m & \mathbf{0}_n \\ Q\backslash\{\mathbf{0}_m\} & \mathbf{1}_{(|Q|-1)\times n} \\ \mathbf{1}_{(|R|-1)\times m} & R\backslash\{\mathbf{0}_n\} \\ \mathbf{1}_m & \mathbf{1}_n \end{array}\right),$$

where $\mathbf{1}_{a\times b}$ is the all-one matrix with a rows and b columns.

Example 16. If $Q = \{00\cdots0, 11\cdots1\} \subseteq \mathbb{F}_2^m$ and $R = \{00\cdots0, 11\cdots1\} \subseteq \mathbb{F}_2^n$, then

$$Q\#R = \{00\cdots0, 11\cdots1\} \subseteq \mathbb{F}_2^{m+n},$$

which is also a powerful set.

The result of combining powerful sets using # is in general not powerful. But there are many cases where it is, and furthermore it can be used to construct nonlinear powerful sets.

Theorem 17. *Let $Q \subseteq \mathbb{F}_2^m$ and $R \subseteq \mathbb{F}_2^n$. Then $Q\#R$ is a powerful set if and only if Q and R are both powerful and one of the following holds:*

(a) one of Q, R consists only of a zero vector and possibly an all-one vector, while the other includes an all-one vector; or

(b) $|Q| = |R|$, and neither Q nor R contains an all-one vector.

Furthermore, if $Q\#R$ is powerful, then $Q\#R$ is nonlinear unless Q and R each consist just of a zero vector and possibly an all-one vector.

Proof. If $X \subseteq [m]$ is nonempty, then the vectors of $Q\#R$ that are 0 on X are precisely the vectors of $Q\backslash\{\mathbf{0}_m\}$ that are 0 on X, each extended by 1s at the end, together with $\mathbf{0}_{m+n}$. The number of these vectors is a power of 2 for all choices of $X \subseteq [m]$ if and only if Q is a powerful set.

Similarly, if $Y \subseteq \{m+1, \ldots, m+n\}$ is nonempty, then the number of vectors of $Q\#R$ that are 0 on Y is a power of 2 for all choices of Y if and only if R is a powerful set.

If $X \subseteq [m]$ and $Y \subseteq \{m+1, \ldots, m+n\}$, with each of X and Y being nonempty, then the only vector that is 0 on $X \cup Y$ is $\mathbf{0}_{m+n}$, so the number is $2^0 = 1$.

Finally, the total number of vectors in $Q\#R$ (corresponding to the empty subset of positions) is

$$1 + (|Q| - 1) + (|R| - 1) + 1 = |Q| + |R|,$$

provided $\mathbf{1}_m \notin Q$ and $\mathbf{1}_n \notin R$. Under this condition, if Q and R are powerful, then $|Q| = |R|$ if and only if $|Q| + |R|$ is a power of 2 if and only if $Q\#R$ is a powerful set.

Now suppose that Q and R are powerful, and either $\mathbf{1}_m \in Q$ or $\mathbf{1}_n \in R$. If just one of these holds then $|Q\#R| = |Q| + |R| - 1$, which is not a power of 2 unless exactly one of $|Q|, |R|$ is 1. (They cannot both be 1, since one of Q, R contains an all-one vector as well.) In that case, the other is some power of 2 other than 1. Suppose without loss of generality that Q contains an all-one vector while R contains only a zero vector. Then $Q\#R$ is equivalent to adding n frames to Q. If both $\mathbf{1}_m \in Q$ and $\mathbf{1}_n \in R$ then $|Q\#R| = |Q| + |R| - 2$. If this is a power of 2, then one of Q, R — suppose R, without loss of generality — consists only of a zero vector and an all-one vector. Again, we find that $Q\#R$ is equivalent to adding n frames to Q. In any case, $Q\#R$ is powerful, by Theorem 6.

We now consider nonlinearity.

If Q and R each consist just of a zero vector and possibly an all-one vector, then $Q\#R$ consists just of the all-0 vector and the all-1 vector, so is trivially linear.

Suppose then that (without loss of generality) Q contains a vector $\mathbf{u}$ that is nonzero and not all-ones. We know that $\mathbf{u}\mathbf{1}_n$ is in $Q\#R$. It is clear that the last n coordinates of $\mathbf{u}\mathbf{1}_n + \mathbf{1}_{m+n}$ are all 0. Since $\mathbf{u} \neq \mathbf{1}_m$ (as $\mathbf{1}_m \notin Q$), $\mathbf{u}\mathbf{1}_n + \mathbf{1}_{m+n} \neq \mathbf{0}_{m+n}$. But $\mathbf{0}_{m+n}$ is the unique vector in $Q\#R$ whose last n coordinates are all 0, which implies that $\mathbf{u}\mathbf{1}_n + \mathbf{1}_{m+n} \notin Q\#R$. Therefore, $Q\#R$ is not a linear space. □

It is interesting to consider the relationship between the rank functions $\rho_Q, \rho_R, \rho_{Q\#R}$ of $Q, R, Q\#R$ respectively, when $|Q| = |R|$ and $Q\#R$ is powerful. Note first that $\dim(Q\#R) = \dim Q + 1 = \dim R + 1$. As for any powerful set, the empty set has rank 0. Now suppose $X, Y \neq \varnothing$, $X \subseteq [m]$ and $Y \subseteq \{m+1, \ldots, m+n\}$. Then $\rho_{Q\#R}(X) = \rho_Q(X) + 1$, since

$$\begin{aligned}
\rho_{Q\#R}(X) &= \dim(Q\#R) - \log_2 |\{\mathbf{y} \in Q\#R \mid y_i = 0 \ \forall i \in X\}| \qquad \text{(by (1.2))} \\
&= \dim(Q) + 1 - \log_2 |\{\mathbf{y} \in Q \mid y_i = 0 \ \forall i \in X\}| \\
&\quad \text{(using } \dim(Q\#R) = \dim Q + 1 \text{ and } X \subseteq [m]) \\
&= \rho_Q(X) + 1.
\end{aligned}$$

Similarly, $\rho_{Q\#R}(Y) = \rho_R(Y) + 1$. Moreover, $\rho_{Q\#R}(X \cup Y) = \dim(Q\#R) = \dim Q + 1 = \dim R + 1$, since every nonzero vector in $Q\#R$ is nonzero either on all of $[m]$ or on all of $\{m+1, \ldots, m+n\}$. In the light of this last observation, we call $Q\#R$ the *mutual framing* of Q and R. That same observation leads to violations of submodularity. Choose Q and R to have dimension $\geqslant 4$ and elements a, b respectively of rank 1, i.e., $\rho_Q(\{a\}) = \rho_R(\{b\}) = 1$. (For example, we could choose Q and R to be linear, of sufficiently large and identical dimensions, of nonzero rank, and having no all-one vector. Then let a, b be any non-loop elements.) Put $X = \{a\}$ and $Y = \{b\}$. Since they are contained in disjoint ground sets, $X \cap Y = \varnothing$. We have

$$\begin{aligned}
\rho_{Q\#R}(X \cap Y) + \rho_{Q\#R}(X \cup Y) &= \rho_{Q\#R}(\varnothing) + \dim Q + 1 \\
&= 0 + \dim Q + 1 \\
&= \dim Q + 1 \\
&> 4,
\end{aligned}$$

while

$$\rho_{Q\#R}(X) + \rho_{Q\#R}(Y) = \rho_Q(X) + 1 + \rho_R(Y) + 1 = 4.$$

Choosing suitable powerful sets of arbitrarily large dimension gives arbitrarily large violations of submodularity, in the sense of arbitrarily large differences and ratios between $\rho_{Q\#R}(X \cap Y) + \rho_{Q\#R}(X \cup Y)$ and $\rho_{Q\#R}(X) + \rho_{Q\#R}(Y)$.

For $Q \subseteq \mathbb{F}_2^n$ and $R \subseteq \mathbb{F}_2^n$, define

$$Q \bullet R := \{\mathbf{v}00 : \mathbf{v} \in Q \cap R\} \cup \{\mathbf{v}01 : \mathbf{v} \in Q \backslash R\} \cup \{\mathbf{v}10 : \mathbf{v} \in R \backslash Q\} \cup \{\mathbf{v}11 : \mathbf{v} \notin Q \cup R\}.$$

We can represent $S = Q \bullet R$ by the matrix

$$S = \left(\begin{array}{c|c} Q \cap R & \mathbf{00} \\ Q \backslash R & \mathbf{01} \\ R \backslash Q & \mathbf{10} \\ \hline \overline{Q \cup R} & \mathbf{11} \end{array}\right),$$

where $\overline{Q \cup R}$ is the complement of $Q \cup R$ in $\mathbb{F}_2^n$.

Theorem 18. *$Q \bullet R$ is also powerful if and only if Q, R and $Q \cap R$ are all powerful.*

Proof. Consider any $X \subseteq [n+2]$. We analyse whether it has the power-of-2 property in the following four cases.

Case 1. If $n+1 \notin X$ and $n+2 \notin X$, then the number of rows which are 0 on X is a power of 2 since the first n columns of S form the linear space $\mathbb{F}_2^n$.

Case 2. If $n+1 \in X$ and $n+2 \in X$, then the rows of S that are 0 on X are precisely those of $Q \cap R$ that are 0 are $X \setminus \{n+1, n+2\}$, each extended by two 0s at the end. The number of these rows is a power of 2 for all such X if and only if $Q \cap R$ is a powerful set.

Case 3. If $n+1 \in X$ and $n+2 \notin X$, we only need to consider the submatrix

$$\left(\begin{array}{c|c} Q \cap R & \mathbf{0} \\ Q \backslash R & \mathbf{0} \end{array}\right).$$

Since $Q = (Q \cap R) \cup (Q \backslash R)$, it follows that Q is a powerful set if and only if the number of rows that are 0 on X is a power of 2 for all such X.

Case 4. If $n+1 \notin X$ and $n+2 \in X$, the argument is similar to Case 3. □

Example 19. Let $n = 3$, and $Q = \{000, 001, 010, 011\}$ and $R = \{000, 011, 101, 111\}$. It is easy to see that Q and R are powerful sets and $Q \cap R = \{000, 011\}$ is also a powerful set. According to the construction in Theorem 18, we have

$$Q \bullet R = \{00000, 01100, 00101, 01001, 10110, 11110, 10011, 11011\}.$$

It is straightforward to verify that $Q \bullet R$ is a powerful set.

Using the cases of the above proof to analyse rank, we find that, for any $X \subseteq [n]$,

$$\begin{aligned} \rho_{Q \bullet R}(X) &= |X|, \\ \rho_{Q \bullet R}(X \cup \{n+1\}) &= n - \dim Q + \rho_Q(X), \\ \rho_{Q \bullet R}(X \cup \{n+2\}) &= n - \dim R + \rho_R(X), \\ \rho_{Q \bullet R}(X \cup \{n+1, n+2\}) &= n - \dim(Q \cap R) + \rho_{Q \cap R}(X). \end{aligned}$$

Remark. Theorem 18 can be extended further, using all possible three-bit extensions of vectors, with three powerful sets P, Q, R with the appropriate intersections also having the power-of-2 property. Then it could be extended to an arbitrary number k of extra bits, with the same number of powerful sets with the required properties being combined.

6 Generation

Recall that a *clutter* (also called a *Sperner family*) is an antichain in 2^E under the subset order.

If $S \subseteq 2^E$ then $S_{\min}$ denotes the set of its minimal nonempty members, which is a clutter.

Theorem 20. *Every powerful set is determined by its minimal nonempty members.*

Proof. Consider the following algorithm, which takes a clutter $S_0 \subseteq 2^E$ as input. We will show that either it detects that there is no powerful set S such that $S_{\min} = S_0$, and rejects S_0, or it computes an indicator function $f : 2^E \to \{0,1\}$ for a set $S = \mathrm{supp} f$ which is the unique powerful set such that $S_{\min} = S_0$ (where $\mathrm{supp} f := \{X \subseteq 2^E \mid f(X) \neq 0\}$).

1. Input: S_0
2. $f(\varnothing) := 1$
3. For each $k = 1, \ldots, n$
   {
4. For each $X \subseteq E$ such that $|X| = k$
   {
5. If $X \in S_0$, then put $f(X) := 1$
6. else if $\sum_{Y \subset X} f(Y) = 1$ // There is no $Y \subseteq X$ such that $Y \in S_0$.
7. $f(X) := 0$ // This uses $X \notin S_0$.
8. else if $\sum_{Y \subset X} f(Y) = 2$ // There is a unique $Y \subset X$ such that $Y \in S_0$.
9. $f(X) := 0$ // To ensure $\sum_{Y \subseteq X} f(Y)$ is a power of 2.
10. else // If we reach here, we know $\sum_{Y \subset X} f(Y) \geqslant 3$.
11. if $\sum_{Y \subset X} f(Y) = 2^i - 1$ for some $i \geqslant 2$
12. $f(X) := 1$ // To ensure $\sum_{Y \subseteq X} f(Y)$ is a power of 2.
13. else // If we reach here, we know $\sum_{Y \subset X} f(Y) \geqslant 4$.
14. if $\sum_{Y \subset X} f(Y) = 2^i$ for some $i \geqslant 2$
15. $f(X) := 0$ // To ensure $\sum_{Y \subseteq X} f(Y)$ is a power of 2.
16. else // $\sum_{Y \subset X} f(Y) \notin \{2^i - 1, 2^i \mid i \in \mathbb{N} \cup \{0\}\}$
17. Reject S_0. It cannot be $S_{\min}$ for any powerful set S.
   }
   }
18. Output f.
19. Accept S_0.

Suppose there exists a powerful set S such that $S_{\min} = S_0$.

We show by induction on k that the above algorithm assigns, to all sets $X \subseteq E$ of size k, the value $f(X) = 1$ if $X \in S$ and $f(X) = 0$ otherwise.

Inductive basis: for $k = 0$, we have $X = \varnothing$, and the algorithm correctly assigns $f(\varnothing) = 1$ (in line 2) since $\varnothing \in S$.

Now let $k \geqslant 1$ and suppose the claim is true for all sizes $< k$, and let X be any set of size k.

If $X \in S_0$, then the first condition of the cascaded if statement (line 5) is satisfied, and the algorithm correctly sets $f(X) = 1$.

Now suppose $X \notin S_0$.

The order in which the algorithm visits the sets in 2^E ensures that it will visit all the proper subsets Y of X before visiting X itself. When it reaches X, it will have already assigned values $f(Y)$ to all $Y \subset X$.

By the inductive hypothesis, $\sum_{Y \subset X} f(Y)$ gives the number of proper subsets of X that belong to S.

So this sum equals 1 if and only if no proper subset of X is in S except for $\varnothing$. In this case, no proper subset of X can be in S_0 either, by definition of S and S_0. So $X \notin S$, else $X \in S_0$. Now, in this case the algorithm takes the second option of the cascaded if statement (line 6) and assigns $f(X) = 0$ (in line 7), which is correct (in that f is the indicator function of S on this set X).

It remains to consider cases where $\sum_{Y \subset X} f(Y) \geqslant 2$, i.e., some nonempty proper subset of X belongs to S.

The sum equals 2 if and only if there is exactly one nonempty proper subset of X in S. In this case, there are exactly two proper subsets of X in S, which is already a power of 2, so for S to be powerful, we must have $X \notin S$. Here the algorithm takes the third option of the cascaded if statement (line 8), and correctly puts $f(X) = 0$ (in line 9).

It remains to consider cases where $\sum_{Y \subset X} f(Y) \geqslant 3$, i.e., the number of proper subsets of X belonging to S is at least 3.

If this quantity is one less than a power of 2, then in order for S to be powerful, we must have $X \in S$, and the algorithm takes the fourth option of the cascaded if statement (lines 10–11) and correctly sets $f(X) = 1$ (in line 12).

If this quantity equals a power of 2, then in order for S to be powerful, we must have $X \notin S$, and the algorithm takes the fifth option of the cascaded if statement (lines 13–14) and correctly sets $f(X) = 0$ (in line 15).

Since we have assumed that S is powerful, we know that the number of proper subsets of X that belong to S must be either a power of 2 or one less than a power of 2. So the above cases cover all possibilities, and the last option of the cascaded if statement (line 16) is never reached. Therefore, we know that the algorithm always assigns the correct value $f(X)$ to X so that f is the indicator function of S on this set X.

Hence the claim is true, by induction.

Therefore, once the algorithm finishes, every $X \subseteq E$ will have been assigned a value $f(X)$, and f will be the indicator function of S.

Since the algorithm is deterministic, it finds (the indicator function of) the unique powerful set S such that $S_{\min} = S_0$.

If there is no powerful set S such that $S_{\min} = S_0$, then the algorithm stops at a smallest set $X \subseteq E$ such that the sum $\sum_{Y \subset X} f(Y) \geqslant 5$ and is neither a power of 2 nor one less than a power of 2. It is impossible for any extension of f that includes X in its domain to be the indicator function of a powerful set. In this case, the algorithm takes the last option of the cascaded if statement (line 16). It does not assign a value to $f(X)$, and it correctly rejects S_0 (in line 17). □

Since a powerful set is determined by its rank function (as noted in §1), and determines its clutter of minimal nonempty members, it follows that this clutter is determined by the

powerful set's rank function. Conversely, the clutter determines the powerful set (by the previous theorem) and hence determines its rank function.

The clutter of minimal nonempty members of a powerful set plays a role analogous to the clutter of cocircuits of a binary matroid. Its members may be thought of as analogues, for powerful sets, of cutsets in graphs.

Some natural questions arise.

1. Can we characterise those clutters that consist of the minimal nonempty members of some powerful set?

2. What fraction of clutters come from powerful sets in this way?

7 Enumeration

Let $p(n)$ be the number of isomorphism classes of powerful sets of order n, and $\tilde{p}(n)$ be the number of isomorphism classes of nonlinear powerful sets of order n. By direct computation, with assistance from Peng Yang and Tingrui Yuan of UESTC, we have determined $p(n)$ and $\tilde{p}(n)$ for $n \leqslant 6$.

n	1	2	3	4	5	6
$p(n)$	2	4	9	25	102	900
$\tilde{p}(n)$	0	0	1	9	70	832

These numbers suggest that the number of powerful sets of order n grows very rapidly as n increases, and that the proportion that are linear shrinks rapidly.

We now show that the number of isomorphism classes of nonlinear powerful sets of order n is doubly exponential in n, and in fact this remains true if we restrict to size 2^{n-2}. It follows that almost all powerful sets are nonlinear.

To do this, we will use another way of combining powerful sets, based on operations previously introduced.

Let $S_1, S_2 \subseteq \mathbb{F}_2^n$ be powerful sets. Define $S_1 \diamond S_2 \subseteq \mathbb{F}_2^{n+3}$ by

$$S_1 \diamond S_2 = (S_1 + \circ) \bullet (S_2 + \square).$$

This construction can be depicted as follows

$$S_1 \diamond S_2 = \left(\begin{array}{c|c|c} 00\cdots0 & 0 & 00 \\ \hline & 0 & 01 \\ S_1\backslash\{\mathbf{0}_n\} & \vdots & \vdots \\ & 0 & 01 \\ \hline & 1 & 10 \\ S_2\backslash\{\mathbf{0}_n\} & \vdots & \vdots \\ & 1 & 10 \\ \hline & & 11 \\ \text{the rest of } \mathbb{F}_2^{n+1} & & \vdots \\ & & 11 \end{array}\right).$$

Theorem 21. *If $S_1, S_2 \subseteq \mathbb{F}_2^n$ are powerful sets, then $S_1 \diamond S_2 \subseteq \mathbb{F}_2^{n+3}$ is also a powerful set.*

Proof. Since S_i (for $i = 1, 2$) is powerful, it follows from Theorem 2 and Theorem 6 respectively that both $S_1 + \circ$ and $S_2 + \square$ are powerful sets. It is clear that $(S_1 + \circ) \cap (S_2 + \square) = \{\mathbf{0}\}$, which is also a powerful set. Now the desired result follows from Theorem 18. □

Proposition 22. *For any nontrivial powerful sets $S_1, S_2 \subseteq 2^E$, the set $S_1 \diamond S_2$ is loopless and frameless.*

Proof. It is clear from the construction that no loops or frames are created, regardless of S_1 and S_2. □

Theorem 23. *Let $\mathcal{S}$ be a set of nonisomorphic loopless frameless powerful sets of order n and size 2^{n-2}. Then*

$$\mathcal{S}^{\diamond 2} := \{S_1 \diamond S_2 \mid S_1, S_2 \in \mathcal{S}\}$$

is a set of nonisomorphic loopless frameless powerful sets of order $n+3$ and size 2^{n+1}. If $n > 3$, then every member of $\mathcal{S}^{\diamond 2}$ is nonlinear.

Proof. Let $S_1, S_2 \in \mathcal{S}$. By Theorem 21, $S_1 \diamond S_2$ is powerful. By Proposition 22, $S_1 \diamond S_2$ is loopless and frameless.

We now show that all the members of $\mathcal{S}^{\diamond 2}$ are nonisomorphic. Suppose, by way of contradiction, that there exist $S_1, S_2, S_1', S_2' \in \mathcal{S}$, with either $S_1 \ncong S_1'$ or $S_2 \ncong S_2'$, such that $S_1 \diamond S_2 \cong S_1' \diamond S_2'$. Let φ be an isomorphism from $S_1 \diamond S_2$ to $S_1' \diamond S_2'$. Now, φ cannot map any element of $[n+1]$ to any element of $\{n+2, n+3\}$, since the column $n+1+i$ has weight $2^{n+1} - |S_i| = 2^{n+1} - 2^{n-2} > 2^n$ (for $i = 1, 2$), while every column indexed by an $e \in [n+1]$ has weight 2^n.

Let $i \in \{1, 2\}$. Since S_i, S_i' are loopless and frameless, $S_i \backslash \{\mathbf{0}\}$ and $S_i' \backslash \{\mathbf{0}\}$ each have no column that is all-0 or all-1, so they each have no column that looks like their portion of column $n+1$, $n+2$ or $n+3$. Therefore $\varphi(n+1) = n+1$. We also see that φ cannot interchange $n+2$ and $n+3$, since the rows where column $n+2$ is 0 are precisely the rows where column $n+1$ is 0, and the rows where column $n+3$ is 0 are precisely the rows where column $n+1$ is 1. So $\varphi(n+2) = n+2$ and $\varphi(n+3) = n+3$.

We have shown that φ maps $[n]$ to itself. Also, for each $i = 1, 2$, the mapping it induces on codewords of $S_1 \diamond S_2$ sends rows corresponding to S_i to rows corresponding to S_i' (else the last three bits of the codewords do not match up). Since (by assumption) φ is an isomorphism from $S_1 \diamond S_2$ to $S_1' \diamond S_2'$, it must induce an isomorphism from S_1 to S_1' and from S_2 to S_2'. Therefore $S_1 \cong S_1'$ and $S_2 \cong S_2'$. This contradicts our assumption that $S_1 \ncong S_1'$ or $S_2 \ncong S_2'$. (In fact, just one $S_i \cong S_i'$ is sufficient to get this contradiction.)

Therefore, all the members of $\mathcal{S}^{\diamond 2}$ are nonisomorphic.

Since $n > 3$, each S_i has at least three nonzero members. Let $\mathbf{x}$ and $\mathbf{y}$ be two nonzero members of S_1. The corresponding vectors in $S_1 \diamond S_2$ have the same final three bits (by construction), so their sum has last three bits all 0. If $S_1 \diamond S_2$ is linear, then this means

that their sum is the $(n+3)$-bit zero vector, since the only vector in $S_1 \diamond S_2$ with last two bits 0 is the zero vector. This implies that $\mathbf{x} + \mathbf{y} = \mathbf{0}$. This can only happen if $\mathbf{x} = \mathbf{y}$, which contradicts the fact that they are distinct nonzero members of S_1. Hence $S_1 \diamond S_2$ cannot be linear. □

Lemma 24. *The number $q(n)$ of isomorphism classes of loopless frameless nonlinear powerful sets of order $n \geqslant 5$ and size 2^{n-2} satisfies $\log_2 \log_2 q(n) \geqslant (n-7)/3$.*

Proof. We use induction on n.

For the base case, observe that there are at least two nonisomorphic loopless frameless nonlinear powerful sets of order 5 and size 2^3. We saw one in Example 13, and another in the Remark following Conjecture 9. It is therefore straightforward to construct two nonisomorphic loopless frameless nonlinear powerful sets of any order k and size 2^{k-2} (for example, using coloop extensions of the two of order 5 we have just mentioned). Therefore, for $k \in \{5, 6, 7\}$, we have $q(k) \geqslant 2$, so $\log_2 \log_2 q(k) \geqslant 0 \geqslant (k-7)/3$.

Now let $n \geqslant 8$, and suppose that $\log_2 \log_2 q(k) \geqslant (k-7)/3$ for all k such that $5 \leqslant k < n$. Let $\mathcal{S}$ be a set containing one representative of each isomorphism class of loopless frameless nonlinear powerful sets of order $n-3$ and size $2^{(n-3)-2} = 2^{n-5}$. By the inductive hypothesis, $|\mathcal{S}| = q(n-3) \geqslant 2^{2^{(n-10)/3}}$. By Theorem 23, $\mathcal{S}^{\diamond 2}$ contains only loopless frameless nonlinear powerful sets of order n and size 2^{n-2}, and they are all nonisomorphic. We therefore have

$$q(n) \geqslant |\mathcal{S}^{\diamond 2}| = |\mathcal{S}|^2 = q(n-3)^2 \geqslant (2^{2^{(n-10)/3}})^2 = 2^{2^{(n-7)/3}}.$$

The result follows by induction. □

For an upper bound on $q(n)$, we can start with the number 2^{2^n} of all sets of subsets of $[n]$. We saw in §6 that a powerful set is determined by its clutter of minimal nonempty members, so $q(n)$ is at most the number of inequivalent clutters of order n. The number of clutters on $[n]$ is at least the number of sets of $\lfloor n/2 \rfloor$-subsets of $[n]$, since any collection of distinct sets all of the same size is a clutter. So the number of clutters is at least $2^{\binom{n}{\lfloor n/2 \rfloor}}$. Since each isomorphism class of clutters has at most $n!$ members, the number of isomorphism classes of clutters is at least $2^{\binom{n}{\lfloor n/2 \rfloor}}/n!$. This eventually exceeds 2^{c^n} for any fixed $c < 2$. It follows that the number of inequivalent clutters does not give us a better upper bound of the form 2^{c^n} than the naïve 2^{2^n}.

The number of isomorphism classes of binary matroids on n elements is well known to satisfy the easy upper bound 2^{n^2}. It follows that, asymptotically, almost all powerful sets are nonlinear.

8 Discussion

We have laid some of the foundations of the theory of powerful sets, but there is much still to be done.

One line of research is to consider aspects of binary matroid theory and determine how far they extend to powerful sets. Most of our work has been of this character, including

our Conjectures 5 and 9. In §6 we proposed the problem of characterising those clutters that are the set of minimal nonempty members of a powerful set, which is analogous to characterising sets of cocircuits of binary matroids. Research could also be done on Tutte-Whitney polynomials of powerful sets, to determine what special properties they have beyond the general results of [2, 3].

Another line of research is to examine the coding-theoretic properties of nonlinear powerful sets (viewed as powerful codes). These are sufficiently general objects that many do not have useful coding properties, but it is reasonable to expect that some classes of them may be useful.

One could examine the relationship between linear codes over $\mathbb{Z}_4$ and the binary codes obtained from them using the Gray map, $0 \mapsto 00, 1 \mapsto 01, 2 \mapsto 11, 3 \mapsto 10$ (as suggested to us by Peter Cameron). This construction does not necessarily give a powerful set, as the following example shows. On the left is a linear code over $\mathbb{Z}_4$ and on the right is the corresponding binary code.

$$\begin{array}{ccc}
000 & \mapsto & \underline{0}0\underline{0}0\underline{0}0 \\
013 & \mapsto & 000110 \\
022 & \mapsto & 001111 \\
031 & \mapsto & 001001 \\
101 & \mapsto & \underline{0}1\underline{0}0\underline{0}1 \\
110 & \mapsto & \underline{0}1\underline{0}1\underline{0}0 \\
123 & \mapsto & 011110 \\
132 & \mapsto & 011011 \\
202 & \mapsto & 110011 \\
211 & \mapsto & 110101 \\
220 & \mapsto & 111100 \\
233 & \mapsto & 111010 \\
303 & \mapsto & 100010 \\
312 & \mapsto & 100111 \\
321 & \mapsto & 101101 \\
330 & \mapsto & 101000
\end{array}$$

For the binary code, the number of vectors that are 0 on $X = \{1, 3, 5\}$ is 3, not a power of 2. (Note the underlined bits.) So the binary code is not powerful. It remains to determine which $\mathbb{Z}_4$-linear codes give nonlinear powerful codes, and what properties they have.

Finally, we suggest the challenge of finding significantly stronger bounds on the number (up to isomorphism) of powerful sets of order n, and determination of

$$\lim_{n\to\infty} (\log_2 p(n))^{1/n}.$$

Acknowledgements

We thank Thomas Britz for helpful comments and drawing our attention to almost affine codes, Yongbin Li for some discussion, Tingrui Yuan and Peng Yang for their assistance with the computations, and the referees for helpful comments. This work was supported by the National Natural Science Foundation of China (No. 11401080).

References

[1] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4:123–134, 1991.

[2] G. E. Farr. A generalization of the Whitney rank generating function. *Math. Proc. Cambridge. Phil. Soc.*, 113:267–280, 1993.

[3] G. E. Farr. Some results on generalised Whitney functions. *Adv. in Appl. Math.*, 32:239–262, 2004.

[4] G. E. Farr. Tutte-Whitney polynomials: some history and generalizations. In: G. R. Grimmett and C. J. H. McDiarmid (eds.), *Combinatorics, Complexity and Chance: A Tribute to Dominic Welsh*, pages 28–52. Oxford University Press, 2007.

[5] J. P. S. Kung. The Rédei function of a relation. *J. Combin. Theory Ser. A*, 29:287–296, 1980.

[6] J. Simonis and A. Ashikhmin. Almost affine codes. *Des. Codes Cryptogr.*, 14:179–197, 1998.

[7] D. J. A. Welsh. Matroid Theory. Academic Press, London, 1976.

[8] D. J. A. Welsh and G. P. Whittle. Arrangements, channel assignments, and associated polynomials. *Adv. in Appl. Math.*, 23:375–406, 1999.

[9] T. Westerbäck, R. Freij-Hollanti, T. Ernvall and C. Hollanti. On the combinatorics of locally repairable codes via matroid theory. *IEEE Trans. Inform. Theory*, 62:5296–5315, 2016.

[10] H. Whitney. The coloring of graphs. *Ann. of Math.*, 33:688–718, 1932.