On Sum Distinct Sets Of Integral Vectors

Dušan B. Jevtić
Department of Computer Engineering
Santa Clara University
Santa Clara, California 95053

ABSTRACT. We study bounds on the cardinality of sum-distinct sets of n-vectors with nonnegative integral components under component-wise real-number addition. A subclass of sum-distinct sets induced by an n by n integral matrix of rank n is studied as well.

1 Introduction

We will be dealing with elements from $\mathcal{K} \triangleq \{0, 1, \ldots, k\}$ where $k \in \mathcal{Z}^+$ and $\mathcal{Z}^+$ is the set of positive integers. Call a set $\{\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_m\}$, $\bar{x}_i \in \mathcal{K}^n$, *sum distinct* in $(\mathcal{K}^n, +)$ if all the 2^m possible sums

$$\alpha_1\bar{x}_1 + \alpha_2\bar{x}_2 + \cdots + \alpha_m\bar{x}_m, \quad \alpha_i \in \{0, 1\}, \tag{1.1}$$

are distinct n-vectors in $\{0, 1, \ldots, mk\}^n$. In (1.1), $+$ stands for a component-wise real-number addition. A *sum-distinct matrix* is any arrangement of the m sum-distinct n-vectors into an n by m $\mathcal{K}$-matrix (matrix whose all entries are from $\mathcal{K}$).

Let C be an n by m $\mathcal{K}$-matrix and let $\bar{u}$ be a vector from $\{0, 1\}^m$. By the above definition, C is sum-distinct if

$$\bar{\epsilon} = C\bar{u}, \tag{1.2}$$

has at most one solution in $\bar{u} \in \{0, 1\}^m$ for any integral n-vector $\bar{\epsilon}$. For the lack of a better term, a procedure which recovers $\bar{u}$ from $\bar{\epsilon}$ in (1.2) will be called *inverse mapping*. If C is sum-distinct, such an algorithm always exists (for example, an exhaustive search through $\mathcal{R}(C) \triangleq \{C\bar{u} \mid \bar{u} \in \{0, 1\}^m\}$).

There are several obvious problems of immediate concern here. For example,

ARS COMBINATORIA 45(1997), pp. 87-95

a) given n and k, what is the largest value of m?

b) how do we construct maximum cardinality sum-distinct sets for given n and k?

c) how do we construct sum-distinct sets whose corresponding inverse mappings have low run-time complexity and modest memory requirements.

d) how many different m-element sum-distinct sets are in $\mathcal{K}^n$?

e) are there objects related to the above defined?

Sum-distinct sets were introduced in 1932 by P. Erdös where (a) was asked for $n = 1$ and $k = 2^\ell$, $\ell \in \mathcal{Z}^+$. Since then, except for $k = 1$, only partial answers to (a) and (b) are known. For $n = 1$, a current conjecture is $m < c + \log_2 k$ where c does not depend on k (some estimates of m may be found in [3] and [7]). For $k = 1$, sum-distinct sets were investigated in relation to coin-weighing problem, e.g. [1], [7], [8], [12], where (b) was used to obtain a lower bound in (a). Also, related to sum-distinct sets are disjoint codes, e.g. [4] and [5], as well as superimposed codes, e.g. [2] and [6]. A partial answer to (c) is given in [5]. For $n = 1$, (d) was addressed in [11]. This, of course, is only a partial compilation of results pertaining to the above questions.

In sections 2 and 3, we state and prove an upper and a lower bound on sum-distinct sets in $(\mathcal{K}^n, +)$, respectively. Residue-type sum-distinct sets are discussed in Section 4. Relevant remarks are given in Section 5.

2 An upper bound

There are 2^m distinct sums (1.1) and no more than $(1 + mk)^n$ n-vectors with components from $\{0, 1, \ldots, mk\}$. Hence if $\{\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_m\}$, $\bar{x}_i \in \mathcal{K}^n$, is to be sum-distinct, we must have $2^m \leq (1 + mk)^n$. Since $m < (1 + k)^n$, it follows that $m < (n^2 + n)\log_2(1 + k)$. By using this upper bound on m and $2^m \leq (1 + mk)^n$ once more, we have

$$m < n\log_2(1 + (n^2 + n)k\log_2(1 + k)). \tag{2.1}$$

Clearly, (2.1) can be further improved by a repeated substitution of the most recent upper bound on m into $2^m \leq (1 + mk)^n$. Next, we generalize a result from [8] to $k > 1$.

Theorem 1. $2^m \leq (\frac{em}{2})^{\frac{n}{2}} k^n m^{\frac{n}{2}}$ *for an* m*-element sum-distinct set in* $(\mathcal{K}^n, +)$.

Proof: Let $\bar{u}$ be a random m-vector with uniform distribution on $\{0,1\}^m$. Then,

$$E\bar{u} = \sum_{\bar{a}\in\{0,1\}^m} \bar{a}P\{\bar{u}=\bar{a}\} = \frac{1}{2^m}\sum_{\bar{a}\in\{0,1\}^m}\bar{a} = \frac{1}{2}\bar{1}_m,$$

where $\bar{1}_m$ is the column m-vector of ones. Furthermore, let $\bar{c} = (c_1,\ldots,c_m)$ where $c_i \in \mathcal{K}$ for all i. Then,

$$\begin{aligned} E(\bar{c}\bar{u} - \bar{c}E\bar{u})^2 &= \sum_{\bar{a}\in\{0,1\}^m}(\bar{c}\bar{a} - \frac{1}{2}\bar{c}\bar{1}_m)^2 P\{\bar{u}=\bar{a}\} \\ &= \frac{1}{2^{m+2}}\sum_{\bar{a}\in\{0,1\}^m}[\bar{c}(2\bar{a}-\bar{1}_m)]^2 = \frac{1}{4}\sum_{i=1}^m c_i^2 \qquad (2.2) \end{aligned}$$

Denote by $H(X)$ the entropy of a random variable X. It can be shown that

$$H(\bar{X}) \le \frac{n}{2}\log 2\pi e(\sigma_1^2\sigma_2^2\cdots\sigma_n^2)^{\frac{1}{n}}, \qquad (2.3)$$

where $\bar{X} = (X_1,\ldots,X_n)$ and $\sigma_i^2 = E(X_i - EX_i)^2$ for $i = 1,\ldots,n$. For proof of (2.3) see, for example, [9].

If $\bar{u}$ in (1.2) is a random variable, so is the subset-sum $\bar{\epsilon}$. Put $P\{\bar{\epsilon} = \bar{z}\} = 0$ for $\bar{z} \notin \mathcal{R}(C)$. Then, $P\{\bar{\epsilon}=\bar{\epsilon}_0\} = P\{\bar{\epsilon} = C\bar{x}_0\} = P\{\bar{u}=\bar{x}_0\}$ since C is sum-distinct. Thus $H(\bar{\epsilon}) = H(\bar{u})$ for any distribution of $\bar{u}$. Denote by $\bar{c}_1,\bar{c}_2,\ldots,\bar{c}_n$ the row vectors of C. Put $X_i = \bar{c}_i\bar{u}$ and by (2.3)

$$\begin{aligned} H(\bar{u}) &= H(\bar{c}_1\bar{u},\bar{c}_2\bar{u},\ldots,\bar{c}_n\bar{u}) \\ &\le \frac{n}{2}\log 2e\pi + \frac{1}{2}\sum_{i=1}^n \log E(\bar{c}_i\bar{u} - \bar{c}_iE\bar{u})^2. \end{aligned}$$

If $\bar{u}$ is assumed to have a uniform distribution on $\{0,1\}^m$, then $H(\bar{u}) = m\log 2$. Theorem follows from (2.2), the above inequality, and the fact that C is a $\mathcal{K}$-matrix. □

By (2.1) and Theorem 1, for an m-element set which is sum-distinct in $(\mathcal{K}^n,+)$,

$$n^{-1}m \le \log_2 k\sqrt{n} + \log_2\sqrt{\frac{e\pi}{2}} + \frac{1}{2}\log_2\log_2[1+(n^2+n)k\log_2(1+k)]. \qquad (2.4)$$

In the sequal, we will show that $n^{-1}m \ge \log_2 k\sqrt{n}$. Hence, $n^{-1}m$ behaves as $\log_2 k\sqrt{n}$ for large values of kn. (The ratio $n^{-1}m$ is an information-theoretic measure of the size of a set which is sum-distinct in $(\mathcal{K}^n,+)$.)

3 A lower bound

A lower bound on the size of sum-distinct sets from $\mathcal{K}^n$ will be obtained by generalizing the construction in [7] to $k > 1$. In the sequal, $\mathcal{N}$ will stand for the set of nonnegative integers, $b(x)$ for the binary equivalent of $x \in \mathcal{N}$, and $d(\bar{z})$ for the decimal equivalent of a binary number $\bar{z}$. The number of 1s in $b(x)$ will be denoted by $\alpha(x)$ and $A(n) \triangleq \sum_{i=1}^{n} \alpha(i)$. Let n be the smallest integer such that $\max(x, y) \leq 2^n - 1$ and let

$$x \cap y \triangleq d(b(x) \wedge b(y)),$$

where $\wedge$ stands for bit-by-bit logical AND. For example, $3 \cap 5 = d((110) \wedge (101)) = d(100) = 1$. Write $x \subset y$ if $x \cap y = x$. For example, $1 \subset 3$ and $1 \subset 5$ but $3 \not\subset 5$. The following result was proved in [7, p. 482].

Lemma 1. *Let $b_0, b_1 \ldots, b_n$ be a sequence of numbers and r a nonnegative integer such that $b_{s \cap r} = b_s$. If $t \not\subset r$, then $\sum_{s \subset t} (-1)^{\alpha(s)} b_s = 0$ for $1 \leq t \leq n$.* □

To any integer r from $\{1, \ldots, n\}$ we associate an n by $t(r,k)$ submatrix $D^{(r)} = (d_{ij}^{(r)})$, $i = 1, \ldots, n$ and $j = 1, \ldots, t(r,k)$, where $t(r,k) \triangleq \lfloor \log_2 k \rfloor + \alpha(r)$. For any fixed r either $i \subset r$ or $i \not\subset r$. If $i \subset r$, choose the $t(r,k)$ entries $d_{ij}^{(r)} \in \mathcal{K}$ so that $d_{0j}^{(r)} = 0$ and

$$\sum_{i \subset r} (-1)^{\alpha(i)+1} d_{ij}^{(r)} = 2^{j-1}, \quad j = 1, 2, \ldots, t(r,k). \tag{3.1}$$

If $i \not\subset r$, define $d_{ij}^{(r)} = d_{i \cap r, j}$ for $j = 1, 2, \ldots, t(r,k)$. Note that the entries $d_{ij}^{(r)} \in \mathcal{K}$ required in (3.1) can always be found since $2^{t(r,k)-1} \leq k 2^{\alpha(r)-1}$ and $\alpha(i)$ is an odd integer for $2^{\alpha(r)-1}$ indices i, $i \subset r$, in the sum (3.1).

We will show that each submatrix $D^{(r)}$ is sum-distinct. Moreover, the n by m matrix

$$D_n \triangleq (D^{(1)} | D^{(2)} | \cdots | D^{(n)}) \tag{3.2}$$

is sum-distinct. The number, m, of sum-distinct column-vectors of D_n is given by

$$m = \sum_{r=1}^{n} t(r,k) = n \lfloor \log_2 k \rfloor + A(n). \tag{3.3}$$

Let $\bar{u} \in \{0,1\}^m$ and $\bar{\epsilon} \in \mathcal{Z}^n$. We will show that $D_n \bar{u} = \bar{\epsilon}$ has a unique solution in $\bar{u}$. Let $\bar{d}_1, \ldots, \bar{d}_n$ be the row vectors of D_n. If we multiply each

$\bar{d}_i$ by $(-1)^{1+\alpha(i)}$ and add them up for all $i \subset r$, due to Lemma 1, equation (3.1) and definition (3.2), we have

$$\sum_{i\subset t}(-1)^{\alpha(i)+1}\epsilon_i = \left(\sum_{i\subset t}(-1)^{\alpha(i)+1}\bar{d}_i\right)\bar{u}$$
$$= \left(2^0, 2^1, \ldots, 2^{t(r,k)-1}\right)\bar{u}_r + \delta_r, \qquad (3.4)$$

where $\bar{u}_r$ is a subvector of $\bar{u}$ that corresponds to submatrix $D^{(r)}$ and δ_r is a known integer. Since $(2^0, 2^1, \ldots, 2^{t(r,k)-1})$ is a sum-distinct vector, the $t(r,k)$ components of $\bar{u}$ are determined uniquely by (3.4).

We illustrate the construction with an example where $n = 4$ and $k = 5$. There are at least $4\lfloor \log_2 5 \rfloor + A(4) = 13$ sum-distinct vectors. A matrix

$$D_4 = \begin{pmatrix} 1 & 2 & 4 & 0 & 0 & 0 & 5 & 0 & 2 & 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 & 0 & 5 & 2 & 4 & 0 & 0 & 0 \\ 1 & 2 & 4 & 1 & 2 & 4 & 4 & 3 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix},$$

obtained by the above procedure, should be sum-distinct. Indeed, let $\bar{u} = (u_1, \ldots, u_{13})^T$ and $\bar{\epsilon} = (\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)^T$. If we premultiply $D_4\bar{u} = \bar{\epsilon}$ by $(1, 1, -1, 0)$, then $\epsilon_1 + \epsilon_2 - \epsilon_3 = (1, 1, -1, 0)D_4\bar{u} = (\bar{0}_6^T | 1, 2, 4, 8 | \bar{0}_3^T)\bar{u}$ and u_7, u_8, u_9 and u_{10} are determined uniquely since $(1, 2, 4, 8)$ is a sum-distinct vector. To obtain the remaining nine components of $\bar{u}$ we use vectors $(0, 0, 0, 1)$, $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$ in the above described way.

Note that 2^{j-1} in (3.1) is taken for the simplicity of notation. Instead of 2^{j-1} we can take any positive integer $q_j^{(r)} \leq k2^{\alpha(r)-1}$ such that the set $\{q_1^{(r)}, q_2^{(r)}, \ldots, q_{h_r}^{(r)}\}$ is sum-distinct. For certain values of r there are classes of sum-distinct sets for which h_r exceeds $t(r,k)$. From $A(2^\ell - 1) = \ell 2^{\ell-1}$ and (3.3), the estimate

$$n^{-1}m \geq \lfloor \log_2 k \rfloor + (1 + n^{-1}) \log_2 \sqrt{1+n}, \qquad n = 2^\ell - 1, \qquad (3.5)$$

follows at once. It was shown in [10] that $A(n) \geq \frac{n+1}{2} \log_2 \frac{3n+3}{4}$ and that this lower bound is met infinitely often for all n such that $|3n - 2^k| = 1$ where $k \in \mathcal{N}$.

4 Residue-type sum-distinct sets

Let B be a regular square matrix of rank n and denote by Λ_B the lattice generated by its column vectors $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n$. The subset of R^n defined by $\theta_1\bar{b}_1 + \theta_2\bar{b}_2 + \cdots + \theta_n\bar{b}_n$, where $0 \leq \theta_i < 1$ for all i, is a *fundamental parallelotope* of B, written as Π_B. Let L be an n by $(m-n)$ $\mathcal{K}$-matrix and

put $C = (B|L)$. Denote by Λ_C a lattice of rank n generated by column-vectors of C. Λ_B is then a *sublattice* of the lattice Λ_C. If $\bar{x}$ and $\bar{y}$ are vectors from Λ_C, then $\bar{x}$ is *congruent to* $\bar{y}$ *modulo* Λ_B, written as $\bar{x} \equiv \bar{y} \pmod{\Lambda_B}$, if the vector $\bar{x} - \bar{y}$ belongs to Λ_B. Two vectors in Λ_C which are congruent modulo Λ_B belong to the same *residue class modulo* Λ_B. The number of different residue classes modulo Λ_B is the *index* of Λ_B in Λ_C and is denoted by $[\Lambda_C : \Lambda_B]$. By a well known result in geometric number theory, $|\det B| = [\Lambda_C : \Lambda_B]$.

It is easy to see that C is sum-distinct if and only if $C\bar{z} = \bar{0}$ implies $\bar{z} = \bar{0}$ for any $\bar{z} \in \{-1, 0, 1\}^m$. If $\bar{z}^T = (\bar{z}_1^T, -\bar{z}_2^T)$, where $\bar{z}_1 \in \{-1, 0, 1\}^n$ and $\bar{z}_2 \in \{-1, 0, 1\}^{m-n}$, then $C\bar{z} = \bar{0}$ implies $B\bar{z}_1 = L\bar{z}_2$ indicating that sum-distinctness can be viewed as a vector congruence problem in lattices generated by column-vectors of B and $(B|L)$. The idea here is to choose n 'long' column-vectors in B such that $|\det B|$ is as large as possible and $(m-n)$ 'short' column-vectors in L such that $L\bar{z}_2 \neq \bar{0}$. Then, it is likely to have $B\bar{z}_1 \neq L\bar{z}_2$. The existence of short vectors in L follows from a result in geometric number theory, which says that there exists a linear transformation $\bar{y} = B\bar{x}$ such that $\bar{x} \in \mathcal{Z}^n$ is a non-zero vector and $\bar{y} = (y_1, \ldots, y_n)^T$ satisfies $y_i \leq |\det B|^{\frac{1}{n}}$ for all i.

Let $t = m - n$ and $C = (B|L)$ and denote by $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_t$ the column-vectors of an n by t $\mathcal{K}$-matrix L. If $\{\bar{b}_1, \ldots, \bar{b}_n, \bar{x}_1 \ldots, \bar{x}_t\}$ is sum-distinct, then none of the 2^t sums

$$\epsilon_1\bar{x}_1 + \epsilon_2\bar{x}_2 + \cdots + \epsilon_t\bar{x}_t, \quad \epsilon_i \in \{0, 1\}, \tag{4.1}$$

is congruent (mod Λ_B) to sums from $\{\bar{b}_1, \ldots, \bar{b}_n\}$. Since sums (4.1) are also incongruent (mod Λ_B) to each other, they must represent different residue classes modulo Λ_B. Each of the 2^t sums (4.1) comes from a different residue class and thus $2^t \leq [\Lambda_C : \Lambda_B]$ or

$$2^t \leq |\det B|. \tag{4.2}$$

Unfortunately, the above reasoning is wrong. The smallest counterexample [1] is obtained for $n = 1$, $k = 7$ and $B = (7)$. Then $2^t \leq 7$ gives $t \leq 2$ which is incorrect since $\{3, 5, 6, 7\}$ is sum-distinct. The point is that $3\epsilon_1 + 5\epsilon_2 + 6\epsilon_3$ do not represent different residue classes modulo 7. (Take $\epsilon_i = 0$ for all i and $\epsilon_i = 1$ for all i.)

Let B be a regular square $\mathcal{K}$-matrix of order n. We will say that $C = (B|L)$ is of *residue type* if C is sum-distinct and if t column vectors of L are inside Π_B.

Theorem 2. *Let $C = (B|L)$ be of residue type and let t be the number of column vectors in L. Then, $t^{-1}2^t \leq |\det B|$. If $|\det B|$ is a prime or a power of two, then $t \geq \lfloor \log_2 |\det B| \rfloor$.*

[1] Any set from class Ω in [5] can be used as a counter example.

Proof: If the 2^t sums in (4.1) are inside Π_B, then $2^t \leq |\det B|$ since $|\det B|$ is the volume of Π_B. Else, since each vector $\bar{x}_i$ in (4.1) is inside Π_B and there are at most t such vectors, by pigeonhole principle, the number of sums in (4.1) cannot exceed $t|\det B|$.

Let $\mathcal{B}$ be the lower triangular equivalent form of B. That is, $\mathcal{B} = B\mathcal{U}$, where $\mathcal{U}$ is a unimodular matrix. Denote by $\bar{\beta}_1, \bar{\beta}_2, \ldots, \bar{\beta}_n$ the column vectors of $\mathcal{B}$ and by $\Pi_{\mathcal{B}}$ the corresponding fundamental parallelotope. Then, $\Lambda_B = \Lambda_{\mathcal{B}}$ and $\Pi_B = \Pi_{\mathcal{B}}$. To each diagonal element β_{ii}, $i = 1, \ldots, n$, of $\mathcal{B}$ we associate a sum-distinct set

$$\Gamma_i = \{\gamma_1^{(i)}, \gamma_2^{(i)}, \ldots, \gamma_{k_i-1}^{(i)}, \gamma_{k_i}^{(i)}\}, \quad \gamma_{k_i}^{(i)} = \beta_{ii},$$

such that $|\gamma_j^{(i)}| < |\beta_{ii}|$ for all $j = 1, \ldots, k_i - 1$ and all elements of Γ_i have the same sign. Let I_n be the identity matrix of order n and denote by $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_n$ its column vectors. To each set Γ_i we associate $\bar{\theta}_{k_i}^{(i)} = \bar{\beta}_i$ and the $(k_i - 1)$ *residual vectors*

$$\bar{\theta}_j^{(i)} = \gamma_j^{(i)}\bar{e}_i + r_{i+1,i}^{(j)}\bar{e}_{i+1} + \cdots + r_{n,i}^{(j)}\bar{e}_n, \quad j = 1, \ldots, k_i - 1,$$

where $r_{i+\ell,i}^{(j)}$ are integers such that $|r_{i+\ell,i}^{(j)}| \leq |\beta_{i+\ell,i}|$ and $r_{i+\ell,i}^{(j)}$ and $\beta_{i+\ell,i}$ have the same sign. This is necessary to keep each $\bar{\theta}_j^{(i)}$ inside Π_B. Then the $(\Sigma_{i=1}^n k_i)$-element set $\cup_{i=1}^n \{\bar{\theta}_j^{(i)} \mid j = 1, \ldots, k_i\}$ is sum-distinct. In other words, the 2^{k_i} possible sums of the ith component $\epsilon_1\bar{\theta}_1^{(i)} + \epsilon_2\bar{\theta}_2^{(i)} + \cdots + \epsilon_{k_i-1}\bar{\theta}_{k_i-1}^{(i)} + \epsilon_{k_i}\bar{\beta}_i$, $\epsilon_i \in \{0, 1\}$, are distinct and each of these sums is incongruent (mod Λ_B) to any other sum from a different component. Hence, we have $t + n \geq \sum_i |\Gamma_i|$. For any positive integer $\ell_i \leq \log_2(1 + |\beta_{ii}|)$, the set $\{2^0, 2^1, \ldots, 2^{\ell_i-1}, |\beta_{ii}|\}$ is sum-distinct. From $|\Gamma_i| \geq \ell_i + 1$ we have $t \geq \sum_i \lfloor \log_2 |\beta_{ii}| \rfloor$ and thus the theorem. □

5 Remarks

Residue-type sum-distinct sets form a subclass of all sum-distinct sets and thus the lower bound in Theorem 2 holds in general. If, for example, B_n in $C = (B_n|L)$ is a $\mathcal{K}$-matrix obtained from an Hadamard matrix [2] H_{n+1} as $B_n = \frac{k}{2}(\bar{1}_n\bar{1}_n^T - C_n)$ where C_n is the core of H_{n+1}, i.e.,

$$H_{n+1} = \begin{pmatrix} 1 & \bar{1}_n^T \\ \bar{1}_n & C_n \end{pmatrix},$$

then $n + \log_2|\det B_n| = n\log_2 k + (n+1)\log_2\sqrt{n+1}$. It is easy to see that D_n in (3.2) is of residue type such that for $n = 2^\ell - 1$ its n 'longest vectors' are column vectors of B_n.

[2] An Hadamard matrix H_n of order n is an n by n matrix with elements $+1$ and -1 such that $H_n^T H_n = nI_n$. A necessary condition for the existence of H_n is that n is either 2 or a multiple of 4.

By Theorem 2, bounds on m are as good as bounds on $|\det B|$. A well known and frequently used one,

$$|\det B|^2 \le \prod_{i=1}^{n}\Big(\sum_{k=1}^{n} b_{ik}^2\Big), \quad B = (b_{ik})_1^n,$$

is due to Hadamard. Since $|b_{ik}| \le k$, from (2.1) and Theorem 2 we find

$$n^{-1}m \le \log_2 k\sqrt{n}+1+n^{-1}\log_2 n+n^{-1}\log_2\log_2 \frac{1+(n^2+n)k\log_2(1+k)}{2}.$$

Thus, for large kn the ratio $n^{-1}m$ behaves as $\log_2 k\sqrt{n}$ in the case of residue-type sum-distinct sets as well. (Note that $\log_2 \sqrt{\frac{e\pi}{2}} \approx 1$ in (2.4).)

Conjecture 1: Let B be a square $\mathcal{K}$-matrix of order n such that $|\det B|$ is maximum for given k and n. Then, there exists a residue type matrix $C = (B|L)$ whose column vectors form a maximum cardinality sum-distinct set in $(\mathcal{K}^n, +)$. □

By the construction in Theorem 2, the vector congruence problem in Λ_B was translated into a componentwise vector congruence problem in a geometrically equivalent lattice Λ_B. It is possible, however, to use this construction to obtain sum-distinct sets with elements from $\mathcal{K}^n$. For example, if $n = 3$ and $k = 1$, from H_{2^2} we obtain

$$C_3 = \begin{pmatrix} -1 & +1 & -1 \\ +1 & -1 & -1 \\ -1 & -1 & +1 \end{pmatrix} \quad \text{and} \quad B_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

By using $B_3\mathcal{U}_3 = \mathcal{B}_3$, the column-equivalent representation $\mathcal{B}_3$ of B_3 is found as

$$\mathcal{B}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & -2 \end{pmatrix} \quad \text{for} \quad \mathcal{U}_3 = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Clearly, the only residual vector in $\Lambda_{\mathcal{B}_3}$ is $\bar{\theta}_1^{(3)} = -\bar{e}_3 = (0\ 0\ -1)^T$. The corresponding residual vector in Λ_{B_3} is obtained as $\bar{\beta}_1 + \bar{\theta}_1^{(3)} = \bar{e}_1$ or as $\bar{\beta}_2 + \bar{\theta}_1^{(3)} = \bar{e}_2$ or as $\bar{\theta}_1^{(3)} - \bar{\beta}_3 = \bar{e}_3$ or as $\bar{\beta}_1 + \bar{\beta}_2 + \bar{\theta}_1^{(3)} = \bar{e}_1 + \bar{e}_2 + \bar{e}_3$. So, from $\mathcal{B}_3$ we obtain four sum-distinct matrices,

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

The example suggests a general approach in design of sum-distinct $\mathcal{K}$-matrices. Let $\mathcal{O}$ be an $(m-n)$ by n matrix whose all elements are zero. If L and $\mathcal{L}$ are matrices of residual column-vectors in lattices Λ_B and $\Lambda_{\mathcal{B}}$,

respectively, then there exist an n by $(m-n)$ integral matrix $\mathcal{W}_B$ and an $(m-n)$ by $(m-n)$ unimodular matrix $\mathcal{U}_R$ such that

$$(\mathcal{B} \mid \mathcal{L}) = (B \mid L) \begin{pmatrix} \mathcal{U} & \mathcal{W}_B \\ \mathcal{O} & \mathcal{U}_R \end{pmatrix}.$$

As illustrated in the example above, vectors in L are obtainable from the ones in $\mathcal{B}$ and $\mathcal{L}$ by means of a unimodular transformation of order m.

References

[1] D.G. Cantor and W.H. Mills, Determination of a subset from certain combinatorial properties, *Canad. J. Math.*, **18** (1966), 42–48.

[2] T. Ericson and L. Györfi, Superimposed codes in R^n, *IEEE Trans. Info. Theory*, **IT-34** no. 4 (1988), 877–880.

[3] P. Erdös, Problems and results in additive number theory, *Colloque sur la Théorie des nombres*, Bruxelles, 1955, Liege and Paris, 1956, pp. 127–137.

[4] P. Erdös and D. Jevtić, Problem 91-2: partial solution, *SIAM Review*, **34**, no. 2 (1992), 309–310.

[5] D. Jevtić, Disjoint uniquely decodable codebooks for noiseless synchronized multiple-access adder channels generated by integer sets, *IEEE Trans. Info. Theory*, **IT-38**, no. 2 (1992), 1142–1146.

[6] W.K. Kautz and R.C. Singleton, Nonrandom binary superimposed codes, *IEEE Trans. Info. Theory*, **IT-10** (1964), 363–377.

[7] B. Lindström, On a combinatorial problem in number theory, *Canad. Math. Bull.*, **8**, no. 4 (1965), 477–490.

[8] B. Lindström, On a combinatory detection problem, *Publ. Hung. Acad. Sci.*, **9** (1964), 195–207.

[9] R.J. McEllice, *The Theory of Information and Coding*, Encyclopedia of Mathematics and its Applications, Addison-Wesley, 1977.

[10] M.D. McIlroy, The number of 1's in binary integers: bounds and extremal properties, *SIAM J. on Computing*, **3**, no. 4 (1974), 255–261.

[11] P. Smith, Problem E 2536:, *Amer. Math. Monthly*, **82**, no. 3 (1975), 300. *Solutions and comments*, **83**, no. 6 (1976), 484.

[12] S. Söderberg and H.S. Shapiro, A combinatory detection problem, *Amer. Math. Monthly*, **70** (1963), 1066–1070.