SCIENCE CHINA
Mathematics

• ARTICLES •

September 2010 Vol. 53 No. 9: 2351–2362
doi: 10.1007/s11425-010-3121-9

A new sieve for distinct coordinate counting

Dedicated to Professor Wang Yuan on the Occasion of his 80th Birthday

LI JiYou[1] & WAN DaQing[2,*]

[1]*Department of Mathematics, Shanghai Jiao Tong University, Shanghai 200240, China;*
[2]*Department of Mathematics, University of California, Irvine, CA 92697-3875, USA*
Email: lijiyou@sjtu.edu.cn, dwan@math.uci.edu

Received July 15, 2009; accepted December 24, 2009; published online April 30, 2010

Abstract We present a new sieve for the distinct coordinate counting problem. This significantly improves the classical inclusion-exclusion sieve for this problem, in the sense that the number of terms is reduced from $2^{\binom{k}{2}}$ to $k!$, and reduced further to $p(k)$ in the symmetric case, where $p(k)$ denotes the number of partitions of k. As an illustration of applications, we give an in-depth study of a basic example arising from coding theory and graph theory.

Keywords sieve, distinct coordinate counting

MSC(2000): 05A15, 11T24

Citation: Li J Y, Wan D. A new sieve for distinct coordinate counting. Sci China Math, 2010, 53(9): 2351–2362, doi: 10.1007/s11425-010-3121-9

1 Introduction

We begin with a general combinatorial setting. Let D be a finite set. For a positive integer k, let $D^k = D \times D \times \cdots \times D$ be the Cartesian product of k copies of D. Let X be a subset of D^k. Every element $x \in X$ can be written in a vector form $x = (x_1, \ldots, x_k)$ with the i-th coordinate $x_i \in D$. Motivated by diverse applications in coding theory and graph theory, we are interested in counting the number of elements in X with distinct coordinates. That is, we would like to count the cardinality of the set

$$\overline{X} = \{(x_1, x_2, \ldots, x_k) \in X \mid x_i \neq x_j, \forall\, i \neq j\}.$$

Traditionally, this is handled by the classical inclusion-exclusion principle. We recall this briefly.

For $1 \leqslant i < j \leqslant k$, let

$$X_{ij} = \{(x_1, x_2, \ldots, x_k) | (x_1, x_2, \ldots, x_k) \in X, x_i = x_j\}.$$

Let $X_{ij}^c = X \backslash X_{ij}$, which is the set difference of X and X_{ij}. By definition, $|\overline{X}| = |\bigcap_{1\leqslant i<j\leqslant k} X_{ij}^c|$. One then applies the following well-known inclusion-exclusion principle.

$$\begin{aligned} |\overline{X}| &= \Big| \bigcap_{1\leqslant i<j\leqslant k} X_{ij}^c \Big| \\ &= |X| - \sum_{1\leqslant i<j\leqslant k} |X_{ij}| + \sum_{1\leqslant i<j\leqslant k, 1\leqslant s<t\leqslant k} |X_{ij} \cap X_{st}| - \cdots + (-1)^{\binom{k}{2}} \Big| \bigcap_{1\leqslant i<j\leqslant k} X_{ij} \Big|. \end{aligned} \tag{1}$$

*Corresponding author

In favorite applications, each term of the above formula admits a nice asymptotic formula and thus one also obtains a nice asymptotic formula for $|\overline{X}|$ if k is small. If k is large which is usually the case in applications, the number of terms in the inclusion-exclusion is $2^{\binom{k}{2}}$ which can easily add up to a total error term which is greater than the main term. In this case, one obtains no information at all about $|\overline{X}|$. This is the major bottle-neck of the inclusion-exclusion. In some cases, weaker information can be obtained by using inequalities. For instance, the idea of Brun sieve gives the lower bound

$$|\overline{X}| \geqslant |X| - \sum_{1\leqslant i<j\leqslant k} |X_{ij}|,$$

which has only $1+\binom{k}{2}$ terms. This is often useful but it can still be restrictive.

Our main new idea for estimating $|\overline{X}|$ is that there is a great deal of cancellations in the above inclusion-exclusion formula, and we can greatly simplify the formula by using the cycle structure of the symmetric group S_k which acts on D^k by permuting its coordinates. In this way, the number of terms is reduced from $2^{\binom{k}{2}}$ to $k!$. In particular, when X is invariant under the action of S_k, the number of terms is further reduced to the partition function $p(k)$, which is roughly $e^{\pi\sqrt{\frac{2}{3}k}}$, significantly smaller than $k!$.

We now describe our main result precisely. For a given permutation $\tau \in S_k$, write its disjoint cycle product as $\tau = (i_1 i_2 \cdots i_{a_1})(j_1 j_2 \cdots j_{a_2}) \cdots (l_1 l_2 \cdots l_{a_s})$ with $1 \leqslant a_i, 1 \leqslant i \leqslant s$. Then, the sign of τ is given by $\mathrm{sign}(\tau) = (-1)^{a_1+\cdots+a_s-s}$. Define

$$X_\tau = \{(x_1, x_2, \ldots, x_k) \in X, x_{i_1} = \cdots = x_{i_{a_1}}, \ldots, x_{l_1} = \cdots = x_{l_{a_s}}\}.$$

Each element of X_τ is said to be of type τ. Thus X_τ is the set of all elements in X of type τ. Now we can state our main formula.

Theorem 1.1. *We have*

$$|\overline{X}| = \sum_{\tau\in S_k} \mathrm{sign}(\tau)|X_\tau|. \tag{2}$$

It is clear that this formula has only $k!$ terms. If X is invariant under the action of S_k, we can collect similar terms in the above formula and this immediately gives

Proposition 1.2. *Let C_k be the set of conjugacy classes of S_k. If X is invariant under the action of S_k, then*

$$|\overline{X}| = \sum_{\tau\in C_k} \mathrm{sign}(\tau)C(\tau)|X_\tau|, \tag{3}$$

where $C(\tau)$ is the number of permutations in S_k conjugate to τ.

The number of terms is now the number of conjugacy classes of S_k, which is given by the partition function $p(k)$. This improvement leads to several significant arithmetic applications in number theory and finite fields. We shall state one of them below. More will be given elsewhere.

Let $D = \mathbf{F}_q$ be a finite field of q elements with characteristic p. Let m be a positive integer. Given $b = (b_1, \ldots, b_m) \in \mathbf{F}_q^m$, let $N_m(k, b)$ be the number of un-ordered k-tuple $x = (x_1, \ldots, x_k)$ with distinct $x_i \in \mathbf{F}_q$ such that

$$1 + b_1 t + \cdots + b_m t^m \equiv \prod_{i=1}^{k}(1 + x_i t)(\mathrm{mod}\, t^{m+1}).$$

A slightly more general situation is to replace the modulus monomial t^{m+1} by a polynomial $f(t) \in \mathbf{F}_q[t]$ of degree $m+1$ and consider the congruence

$$1 + b_1 t + \cdots + b_m t^m \equiv \prod_{i=1}^{k}(1 + x_i t)(\mathrm{mod}\, f(t)).$$

Our method works in this more general situation as well. For simplicity of illustration, in this paper we restrict to the case $f(t) = t^{m+1}$. We are interested in when $N_m(k, b) > 0$ and when there is a good asymptotic formula. This problem arises from several applications in coding theory [1, 3, 4, 10]. In graph theory, it reduces to the study of the girth of Chung's graph [6], which has been studied extensively in the literature.

For instance, using the Lang-Weil estimate, Katz [8] showed that if $m \leqslant k-2$ and q is sufficiently large, then $N_m(k,b) > 0$ for all $b \in \mathbf{F}_q^m$. The key is to prove that a certain surface over $\mathbf{F}_q$ is absolutely irreducible. Using a suitable effective Chebatarev density theorem of function fields, Cohen [7] showed more precisely that if $m \leqslant k-2$ and $q > (k(k+2)!)^2$, then $N_m(k,b) > 0$ for all $b \in \mathbf{F}_q^m$. Note that the assumption on q is that it is at least exponential in k. That is, k is very small compared to q. This is something that cannot be avoided if m is very close to $k-2$. In coding theory applications [4, 5], one would like to have the situation that q is linear in k (corresponding to the condition that the information rate is positive) and m can be somewhat smaller but not too much smaller. In this case, k is necessarily large and we can try to apply our new sieving formula. Again a simple heuristic argument shows that the main term for $N_m(k,b)$ is $\binom{q}{k}/q^m$. The key is its error term. In this direction, using our new sieve formula and Weil's bound for character sums, we obtain

Theorem 1.3. *For all $b \in \mathbf{F}_q^m$, we have*

$$\left| N_m(k,b) - \frac{1}{q^m}\binom{q}{k} \right| \leqslant \binom{q/p + (m-1)\sqrt{q} + k - 1}{k}.$$

As a corollary, we obtain

Theorem 1.4. *For any $\epsilon > 0$, there is a constant $c_\epsilon > 0$ such that if $m < \epsilon k^{1/2}$ and $4\epsilon^2 \ln^2 q < k \leqslant c_\epsilon q$, then $N_m(k,b) > 0$ for all $b \in \mathbf{F}_q^m$.*

In the special case when q is a square, this type of theorem was first proved in [4, 5] by using the Brun sieve, Weil's bound and a dual argument. The general q case was raised as an open problem. This is completely solved in the present paper. Note that q can be linear in k in the above theorem, as desired in coding theory applications. A further more important open problem is if the condition $m < \epsilon k^{1/2}$ can be improved to $m < \epsilon k^c$ for some absolute constant $c > 1/2$ (and hopefully c can be taken to be close to 1). This problem has a major application in coding theory [5].

In the easier special case $m = 1$, the number

$$N_1(k,b) = \sharp\{\{x_1, x_2, \ldots, x_k\} \subseteq D \mid x_1 + x_2 + \cdots + x_k = b\}$$

is simply the number of subsets of $\mathbf{F}_q$ with cardinality k and with sum equal to b. Our inequality above reduces to

$$\left| N_1(k,b) - \frac{1}{q}\binom{q}{k} \right| \leqslant \binom{q/p + k - 1}{k}.$$

In this special case, a much more precise result is known. We have

Theorem 1.5. *If $p \nmid k$, then*

$$N_1(k,b) = \frac{1}{q}\binom{q}{k}.$$

If $p \mid k$, then

$$N_1(k,b) = \frac{1}{q}\binom{q}{k} + (-1)^{k+\frac{k}{p}}\frac{v(b)}{q}\binom{q/p}{k/p},$$

where $v(b) = -1$ if $b \neq 0$, and $v(b) = q-1$ if $b = 0$.

This explicit formula was first proved by the authors [9] using a sophisticated inductive argument. It can now be proved in a much simpler way using our new sieve formula. It also shows that the unpleasant factor q/p cannot be dropped from the error estimate of $N_m(k,b)$.

Remarks. The Eratostheses sieve over the integers is the starting point for the study of many fundamental problems in classical analytic number theory such as the Goldbach conjecture. The Eratostheses sieve is also some sort of inclusion-exclusion principle. Its subsequent improvements by Brun, Selberg and others led to lots of fruitful progresses on many of these problems. In particular, Professor Yuan Wang had worked on improving these sieves during the period 1953–1957, and he was able to prove the so-called "$2+3$" version of the Goldbach conjecture, that is, every sufficiently large positive even integer is a sum of two positive integers both greater than 1 such that one of them is a product of at most two

primes and the other is a product of at most three primes [13]. He also proved the conditional "$1+3$" version of the Goldbach conjecture, assuming GRH. The GRH assumption can be removed with the later introduction of the Vinogradov-Bombieri large sieve. This line of research culminates in Chen's proof of "$1+2$", which is still the best result today on the Goldbach conjecture. It would be interesting to explore if these sophisticated sieve techniques from analytic number theory can be used to refine our results on the distinct coordinate counting problem, and vice versa.

2 The main theorem and its weighted version

In this section, we prove our main sieve formula and state a weighted version which will be needed in later applications.

Let D be a finite set, and let $D^k = D \times D \times \cdots \times D$ be the Cartesian product of k copies of D. Let X be a subset of D^k. Recall that we are interested in counting the number of elements in the set

$$\overline{X} = \{(x_1, x_2, \ldots, x_k) \in X \mid x_i \neq x_j, \forall\, i \neq j\}.$$

Let S_k be the symmetric group on $\{1, 2, \ldots, k\}$. Each permutation $\tau \in S_k$ factorizes uniquely (up to the order of the factors) as a product of disjoint cycles and each fixed point is viewed as a trivial cycle of length 1. For simplicity of the notation, we usually omit the 1-cycles. For instance, (12) denotes the permutation $(12)(3)(4)\cdots(k)$ in S_k. Two permutations in S_k are conjugate if and only if they have the same type of cycle structure (up to the order). Let C_k be the set of conjugacy classes of S_k. For a given $\tau \in S_k$, let $l(\tau)$ be the number of cycles of τ including the trivial cycles. Then $\operatorname{sign}(\tau) = (-1)^{k-l(\tau)}$. For a given permutation

$$\tau = (i_1 i_2 \cdots i_{a_1})(j_1 j_2 \cdots j_{a_2}) \cdots (l_1 l_2 \cdots l_{a_s})$$

with $1 \leqslant a_i, 1 \leqslant i \leqslant s$, define

$$X_\tau = \left\{(x_1, \ldots, x_k) \in X, x_{i_1} = \cdots = x_{i_{a_1}}, \ldots, x_{l_1} = \cdots = x_{l_{a_s}}\right\}. \tag{4}$$

Each element of X_τ is said to be of type τ. Thus X_τ is the set of all elements in X of type τ. Our main formula is

Theorem 2.1. *We have*

$$|\overline{X}| = \sum_{\tau \in S_k} \operatorname{sign}(\tau) |X_\tau|. \tag{5}$$

Proof. By equation (1), we have

$$|\overline{X}| = |X| - \sum_{1 \leqslant i < j \leqslant k} |X_{ij}| + \sum_{1 \leqslant i < j \leqslant k, 1 \leqslant s < t \leqslant k} |X_{ij} \cap X_{st}| - \cdots + (-1)^{\binom{k}{2}} \left| \bigcap_{1 \leqslant i < j \leqslant k} X_{ij} \right|. \tag{6}$$

Define a partial order "$\leqslant$" on S_k as follows: $\tau \leqslant \delta$ if each cycle in τ as a set is contained in a cycle in δ. For instance, $(12)(34)(567) \leqslant (1234)(567)$ and $(123) \leqslant (132)$.

Case 1. For $x \in \overline{X}$, $x \notin X_\tau$ for each τ with $\tau \neq 1$. Thus x occurs on both sides of (6) with multiplicity 1.

Case 2. For $x \notin \overline{X}$, then $x \in X_\tau$ for a maximal non-trivial τ with respect to the order $\leqslant$. Suppose $\tau = \tau_1 \tau_2 \cdots \tau_r$, where τ_i are disjoint cycles. Then x occurs on the right side of (6) with multiplicity

$$\sum_{\delta \leqslant \tau} \operatorname{sign}(\delta) \cdot 1 = \prod_{j=1}^{r} \left(\sum_{\delta_j \leqslant \tau_j} \operatorname{sign}(\delta_j) \right) = 0. \qquad \square$$

Now the symmetric group S_k acts on D^k by permuting coordinates. That is, for given $\tau \in S_k$ and $x = (x_1, x_2, \ldots, x_k) \in D^k$ we have $\tau \circ x = (x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(k)})$. Before stating some useful corollaries, we first give several definitions.

Definition 2.2. *Let G be a subgroup of S_k. A subset $X \subset D^k$ is said to be G-symmetric if for any $x \in X$ and any $g \in G$, $g \circ x \in X$. In particular, a S_k-symmetric X is simply called symmetric.*

Definition 2.3. *Let G be a subgroup of S_k. Two permutations τ_1 and τ_2 in S_k are said to be G-conjugate if there is $g \in G$ such that $\tau_2 = g\tau_1 g^{-1}$. Let G_k be the set of G-conjugacy classes of S_k.*

Corollary 2.4. *Let G_k be the set of G-conjugacy classes of S_k. If X is G-symmetric, then we have*

$$|\overline{X}| = \sum_{\tau \in G_k} \operatorname{sign}(\tau) G(\tau) |X_\tau|, \tag{7}$$

where $G(\tau)$ is the number of permutations in S_k which is G-conjugate to τ.

Proof. Suppose that two permutations τ_1 and τ_2 are G-conjugate, say $\tau_2 = g\tau_1 g^{-1}$, where $g \in G$. Then one checks that it is a one to one correspondence from X_{τ_1} to X_{τ_2} by sending $(x_1, x_2, \ldots, x_k)$ to $(x_{g(1)}, x_{g(2)}, \ldots, x_{g(k)})$. Hence $|X_{\tau_1}| = |X_{\tau_2}|$ and the formula follows from Theorem 2.1. □

The number of terms in the above formula depends on the size of G-conjugacy classes. If X has more symmetry, that is, G is bigger, then there are fewer number of terms. In many interesting cases, X is symmetric, that is, X is invariant under the action of $G = S_k$. Even more, X sometimes satisfies the "strongly symmetric" condition, that is, for any τ and τ' in S_k, one has $|X_\tau| = |X_{\tau'}|$ provided $l(\tau) = l(\tau')$. In this case, X is called strongly symmetric. Before stating the simplest formula in the strongly symmetric case, we recall some basic combinatorial facts about the symmetric group S_k.

A permutation $\tau \in S_k$ is said to be of type $(c_1, c_2, \ldots, c_k)$ if τ has exactly c_i cycles of length i. Note that $\sum_{i=1}^k ic_i = k$. We denote by $N(c_1, c_2, \ldots, c_k)$ the number of permutations in S_k of type $(c_1, c_2, \ldots, c_k)$ and we have [11]:

$$N(c_1, c_2, \ldots, c_k) = \frac{k!}{1^{c_1} c_1! 2^{c_2} c_2! \cdots k^{c_k} c_k!}. \tag{8}$$

Let C_k be the set of conjugacy classes of S_k. For given $\tau \in S_k$, denote by $\overline{\tau}$ the conjugacy class determined by τ and it can also be viewed as the set of permutations conjugate to τ. Conversely, for given conjugacy class $\overline{\tau} \in C_k$, denote by τ a representative permutation of this class. Sometimes we also identify these two symbols.

Let $C(\tau)$ be the number of permutations conjugate to τ. Let τ be of type $(c_1, c_2, \ldots, c_k)$. Since in S_k two permutations are conjugate if and only if they have the same type, we have $C(\tau) = N(c_1, c_2, \ldots, c_k)$.

The signless Stirling number of the first kind $c(k, i)$ is defined to be the number of permutations in S_k with exactly i cycles. It can also be defined by the following classic equality [11]:

$$\sum_{i=0}^{k} (-1)^{k-i} c(k, i) q^i = (q)_k, \tag{9}$$

where $(x)_k = x(x-1)\cdots(x-k+1)$ for $k \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ and $(x)_0 = 1$.

Now we state the following simpler formula.

Proposition 2.5. *Let C_k be the set of conjugacy classes of S_k. If X is symmetric, then*

$$|\overline{X}| = \sum_{\tau \in C_k} (-1)^{k-l(\tau)} C(\tau) |X_\tau|, \tag{10}$$

where $C(\tau)$ is the number of permutations conjugate to τ. Furthermore, if X is strongly symmetric, then we have

$$|\overline{X}| = \sum_{i=1}^{k} (-1)^{k-i} c(k, i) |X_i|, \tag{11}$$

where X_i is defined as X_{τ_i} for some $\tau_i \in S_k$ with $l(\tau_i) = i$ and $c(k, i)$ is the signless Stirling number of the first kind.

For simplicity and clarity, we have restricted ourselves to the simpler point counting version. There is a natural weighted version which is also very useful in counting points with weight. Now we extend all above formulas to the general weighted case. We omit the proof since it is completely similar.

Let $f(x_1, x_2, \ldots, x_k)$ be a complex valued function defined over X. Many problems arising from coding theory, additive number theory and number theory are reduced to evaluate the summation

$$F = \sum_{x \in \overline{X}} f(x_1, x_2, \ldots, x_k). \tag{12}$$

Note that if we let $f(x_1, x_2, \ldots, x_k) \equiv 1$, then F is just the number of elements in $\overline{X}$. Similarly for $\tau \in S_k$, we define

$$F_\tau = \sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k).$$

The weighted version of our sieve formula then becomes

Theorem 2.6. *We have*

$$F = \sum_{\tau \in S_k} \mathrm{sign}(\tau) F_\tau. \tag{13}$$

Definition 2.7. *Let G be a subgroup of S_k. A complex-valued function f defined on X is called G-normal on X if X is G-symmetric and for any two G-conjugate elements τ and τ' in S_k, we have*

$$\sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k) = \sum_{x \in X_{\tau'}} f(x_1, x_2, \ldots, x_k).$$

If f is S_k-normal on X, then f is also called normal on X.

The function f on X is called strongly normal on X if X is symmetric and for each τ and τ' in S_k, we always have

$$\sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k) = \sum_{x \in X_{\tau'}} f(x_1, x_2, \ldots, x_k)$$

whenever $l(\tau) = l(\tau')$.

Remark. If $f(x_1, x_2, \ldots, x_k)$ is a symmetric function and X is symmetric, then $f(x_1, x_2, \ldots, x_k)$ must be normal on X.

Proposition 2.8. *Let C_k be the set of conjugacy classes of S_k. If f is normal on X, then we have*

$$F = \sum_{\tau \in C_k} (-1)^{k-l(\tau)} C(\tau) F_\tau, \tag{14}$$

where $C(\tau)$ is the number of permutations conjugate to τ.

If f is strongly normal on X, for given $1 \leqslant i \leqslant k$, we choose $\tau_i \in S_k$ satisfying $l(\tau_i) = i$, and let

$$F_i = \sum_{x \in X_{\tau_i}} f(x_1, x_2, \ldots, x_k)$$

(this is independent of the choice of τ_i), then we have

$$F = \sum_{i=1}^{k} (-1)^{k-i} c(k, i) F_i, \tag{15}$$

where $c(k, i)$ is the signless Stirling number of the first kind, that is, the number of permutations in S_k with exactly i cycles.

3 Proof of Theorem 1.5

In this section, we explain how the main theorem can be used to prove the explicit formula in Theorem 1.5. We first state the following lemma.

Lemma 3.1. *Assume $p \mid k$. Let $p(k, i)$ be the number of permutations in S_k of i cycles with the length of its each cycle divisible by p. Then we have*

$$\sum_{i=1}^{k} (-1)^{k-i} p(k, i) q^i = (-1)^{k+\frac{k}{p}} k! \binom{q/p}{k/p}. \tag{16}$$

Proof. Let $N(c_1, c_2, \ldots, c_k)$ be the number of permutations in S_k of type $(c_1, c_2, \ldots, c_k)$. Recall we have the following counting formula

$$N(c_1, c_2, \ldots, c_k) = \frac{k!}{1^{c_1}c_1!2^{c_2}c_2!\cdots k^{c_k}c_k!}. \tag{17}$$

Define the generating function

$$C_k(t_1, t_2, \ldots, t_k) = \sum_{\sum ic_i = k} N(c_1, c_2, \ldots, c_k) t_1^{c_1} t_2^{c_2} \cdots t_k^{c_k} \tag{18}$$

and from (17) we have

$$C_k(t_1, t_2, \ldots, t_k) = \sum_{\sum ic_i = k} \frac{k!}{c_1!c_2!\cdots c_k!} \left(\frac{t_1}{1}\right)^{c_1} \left(\frac{t_2}{2}\right)^{c_2} \cdots \left(\frac{t_k}{k}\right)^{c_k}.$$

Thus we obtain the following exponential generating function

$$\sum_{k \geqslant 0} C_k(t_1, t_2, \ldots, t_k) \frac{u^k}{k!} = e^{ut_1 + u^2 \cdot \frac{t_2}{2} + u^3 \cdot \frac{t_3}{3} + \cdots}.$$

Let $p_k(t) = \sum p(k,i)t^i$. By (18) we have $p_k(t) = C_k(0, 0, \ldots, t, 0, \ldots)$, where t appears at the indices divisible by p. For given generating function $f(x)$, denote by $[x^i]f(x)$ the coefficient of x^i in the formal power series expansion of $f(x)$. Then we have

$$p_k(t) = \left[\frac{u^k}{k!}\right] e^{t(\frac{u^p}{p} + \frac{u^{2p}}{2p} + \cdots)} = \left[\frac{u^k}{k!}\right] e^{-\frac{t}{p}\log(1-u^p)} = \left[\frac{u^k}{k!}\right] \frac{1}{(1-u^p)^{t/p}}.$$

Thus,

$$p_k(-q) = \left[\frac{u^k}{k!}\right] (1-u^p)^{q/p} = (-1)^{\frac{k}{p}} \binom{q/p}{k/p} k!.$$

Hence (16) follows from $\sum_{i=1}^{k} (-1)^{k-i} p(k,i) q^i = (-1)^k p_k(-q)$. The proof is complete. □

Proof of Theorem 1.5. Let X be the set of all solutions of the equation $x_1 + x_2 + \cdots + x_k = b$ in $\mathbf{F}_q$. Let

$$X_{ij} = \left\{(x_1, x_2, \ldots, x_k) \middle| (x_1, x_2, \ldots, x_k) \in X, x_i = x_j\right\}.$$

Since X is symmetric, by applying Proposition 1.2 we have

$$k! \cdot N_1(k,b) = \left| \bigcap_{1 \leqslant i < j \leqslant k} {X_{ij}}^c \right| = \sum_{\tau \in C_k} (-1)^{k-l(\tau)} C(\tau) |X_\tau|, \tag{19}$$

where $|X_\tau|$ is defined as in (4).

In particular, when $p \nmid k$, one checks that X is strongly symmetric. Since $x_1 + x_2 + \cdots + x_k = b$ is linear, it is easy to check that when $p \nmid k$ we always have $|X_\tau| = q^{l(\tau)-1}$, where $l(\tau)$ is the number of cycles of τ. Thus by Proposition 1.2 we conclude

$$\begin{aligned} N_1(k,b) &= \frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} c(k,i) |X_i| = \frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} c(k,i) q^{i-1} \\ &= \frac{1}{q} \frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} c(k,i) q^i = \frac{1}{q} \frac{1}{k!} (q)_k = \frac{1}{q} \binom{q}{k}. \end{aligned}$$

When $p \mid k$, denote CP_k to be the conjugacy classes in C_k whose every cycle length is divisible by p. Then by (19) we have

$$k! \cdot N_1(k,b) = \sum_{\tau \in C_k} (-1)^{k-l(\tau)} C(\tau) |X_\tau| = \sum_{\tau \notin CP_k} (-1)^{k-l(\tau)} C(\tau) |X_\tau| + \sum_{\tau \in CP_k} (-1)^{k-l(\tau)} C(\tau) |X_\tau|. \tag{20}$$

If there is at least one cycle of τ such that the length of it is not divisible by p, then we still have $|X_\tau| = q^{l(\tau)-1}$. Otherwise, since $p \mid k$, $|X_\tau| = 0$ if $b \neq 0$ and $|X_\tau| = q^{l(\tau)}$ if $b = 0$. In other words, unless each cycle length of τ is divisible by p, $|X_\tau|$ relies only on $l(\tau)$.

Recall that the signless Stirling number of the first kind $c(k,i)$ is defined to be the number of permutations in S_k with exactly i cycles. Let $p(k,i)$ be the number of permutations in S_k of i cycles with the length of its each cycle divisible by p. Let $s(k,i) = c(k,i) - p(k,i)$. Thus we have

$$\begin{aligned} N_1(k,b) &= \frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}s(k,i)q^{i-1} + \frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}p(k,i)|X_i| \\ &= \frac{1}{q}\frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}(c(k,i)q^i - p(k,i)q^i) + \frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}p(k,i)|X_i| \\ &= \frac{1}{q}\binom{q}{k} - \frac{1}{q}\frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}p(k,i)q^i + \frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}p(k,i)|X_i|. \end{aligned}$$

If $b \neq 0$, then we have $|X_i| = 0$ for each i and thus

$$N_1(k,b) = \frac{1}{q}\binom{q}{k} - \frac{1}{q}\frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}p(k,i)q^i.$$

If $b = 0$, then we have $|X_i| = q^i$, and hence

$$\begin{aligned} N_1(k,b) &= \frac{1}{q}\binom{q}{k} - \frac{1}{q}\frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}p(k,i)q^i + \frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}p(k,i)q^i \\ &= \frac{1}{q}\binom{q}{k} + \frac{q-1}{q}\frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}p(k,i)q^i. \end{aligned}$$

Thus it suffices to evaluate $\sum_{i=1}^{k}(-1)^{k-i}p(k,i)q^i$ and the theorem follows from (16). Hence the proof is complete. □

4 Some combinatorial formulas

For the purpose of our proof, we will need a few combinatorial formulas and inequalities.

Lemma 4.1. *Let $N(c_1, c_2, \ldots, c_k)$ be the number of permutations in S_k of type $(c_1, c_2, \ldots, c_k)$, that is,*

$$N(c_1, c_2, \ldots, c_k) = \frac{k!}{1^{c_1}c_1!2^{c_2}c_2!\cdots k^{c_k}c_k!},$$

and define the generating function

$$C_k(t_1, t_2, \ldots, t_k) = \sum_{\sum ic_i = k} N(c_1, c_2, \ldots, c_k)t_1^{c_1}t_2^{c_2}\cdots t_k^{c_k}.$$

If $t_1 = t_2 = \cdots = t_k = q$, then we have

$$C_k(q, q, \ldots, q) = \sum_{\sum ic_i = k} N(c_1, c_2, \ldots, c_k)q^{c_1}q^{c_2}\cdots q^{c_k} = (q+k-1)_k. \tag{21}$$

In another case, suppose $q \geqslant d$ and $d|(q-s)$, if $t_i = q$ for $d \mid i$ and $t_i = s$ for $d \nmid i$, then we have

$$\begin{aligned} C_k(\overbrace{s, \ldots, s}^{d-1}, q, \overbrace{s, \ldots, s}^{d-1}, q, \ldots) &= \sum_{\sum ic_i = k} N(c_1, c_2, \ldots, c_k)q^{c_1}q^{c_2}\cdots s^{c_d}q^{c_{d+1}}\cdots \\ &= k!\sum_{i=0}^{\lfloor k/d \rfloor}\binom{\frac{q-s}{d}+i-1}{\frac{q-s}{d}-1}\binom{s+k-di-1}{s-1}. \end{aligned} \tag{22}$$

Proof. Firstly, note that we have the following exponential generating function

$$\sum_{k\geqslant 0} C_k(t_1,t_2,\ldots,t_k)\frac{u^k}{k!} = e^{ut_1+u^2\cdot\frac{t_2}{2}+u^3\cdot\frac{t_3}{3}+\cdots}.$$

Then, when $t_1=t_2=\cdots=t_k=q$, we deduce that

$$\begin{aligned} C_k(q,q,\ldots,q) &= \left[\frac{u^k}{k!}\right] e^{q(u+\frac{u^2}{2}+\frac{u^3}{3}+\cdots)} = \left[\frac{u^k}{k!}\right] e^{-q\log(1-u)} = \left[\frac{u^k}{k!}\right]\frac{1}{(1-u)^q} \\ &= \left[\frac{u^k}{k!}\right]\binom{q+k-1}{k}u^k = (q+k-1)_k. \end{aligned}$$

Similarly, if $t_i=q$ when $d\mid i$ and $t_i=s$ for $d\nmid i$, then we have

$$\begin{aligned} C_k(\overbrace{s,\ldots,s}^{d-1},q,\overbrace{s,\ldots,s}^{d-1},q,\ldots) &= \left[\frac{u^k}{k!}\right] e^{us+u^2\cdot\frac{s}{2}+\cdots+u^{d-1}\cdot\frac{s}{d-1}+u^d\cdot\frac{q}{d}+u^{d+1}\cdot\frac{s}{d+1}\cdots} \\ &= \left[\frac{u^k}{k!}\right] e^{-s\log(1-u)-\frac{q-s}{d}\log(1-u^d)} = \left[\frac{u^k}{k!}\right]\frac{1}{(1-u)^s(1-u^d)^{(q-s)/d}} \\ &= \left[\frac{u^k}{k!}\right]\left(\sum_{j\geqslant 0}\binom{s-1+j}{j}u^j\right)\left(\sum_{i\geqslant 0}\binom{(q-s)/d+i-1}{i}u^{di}\right) \\ &= k!\sum_{i\geqslant 0}\binom{(q-s)/d-1+i)}{(q-s)/d-1}\binom{s+(k-di)-1}{s-1}. \end{aligned}$$

Lemma 4.2. *For given positive integers m, n, q and l, we have*

$$\sum_{i\geqslant 0}\binom{l+i}{n}\binom{q-i}{m} \leqslant \binom{l+q+1}{m+n+1}. \tag{23}$$

Proof. Note that for integer $a\geqslant 0$,

$$\sum_{j=0}^{\infty}\binom{a+j}{a}x^j = (1-x)^{-a-1}.$$

Comparing the coefficients of $x^{l+q-m-n}$ on both sides of $(1-x)^{-m-n-2}=(1-x)^{-m-1}(1-x)^{-n-1}$ we obtain that, for non-negative integers m,n,l,q,

$$\sum_{i+j=l+q-m-n}\binom{m+i}{m}\binom{n+j}{n} = \binom{l+q+1}{m+n+1}.$$

Therefore the required equality follows.

Proposition 4.3. *For given positive integers s,d,k with $q\geqslant s$ and $d|(q-s)$, we have*

$$\begin{aligned} \sum_{i\geqslant 0}\binom{(q-s)/d+i-1)}{(q-s)/d-1}\binom{s+k-di-1}{s-1} &\leqslant \sum_{i\geqslant 0}\binom{(q-s)/d+i-1)}{(q-s)/d-1}\binom{s+k-i-1}{s-1} \\ &\leqslant \binom{s+k+(q-s)/d-1}{k}. \end{aligned} \tag{24}$$

5 Proof of Theorem 1.3

For our proof, we need Weil's character sum estimate in the following form.

Lemma 5.1 [12]. *Suppose we are given a finite commutative $\mathbf{F}_q$-algebra A, an element $t \in A$, and a character χ of the multiplicative group A^* (extended by zero to all of A) which is non-trivial on $\mathbf{F}_q[t]$. Let n denote the dimension of A as $\mathbf{F}_q$-vector space. Then,*

$$\left| \sum_{a \in \mathbf{F}_q} \chi(a+t) \right| \leqslant (n-1)\sqrt{q}. \tag{25}$$

Moreover, if $n \geqslant 2$, $\chi \neq 1$ and $\chi(\mathbf{F}_q^*) = 1$, then

$$\left| 1 + \sum_{a \in \mathbf{F}_q} \chi(a+t) \right| \leqslant (n-2)\sqrt{q}. \tag{26}$$

We can now start the proof. Let m be a positive integer. Given $b = (b_1, \ldots, b_m) \in \mathbf{F}_q^m$, let $N_m(k, b)$ (resp. $M_m(k, b)$) be the number of un-ordered (resp. ordered) k-tuple $x = (x_1, \ldots, x_k)$ with distinct $x_i \in \mathbf{F}_q$ such that

$$1 + b_1 t + \cdots + b_m t^m \equiv \prod_{i=1}^{k} (1 + x_i t) (\mathrm{mod}\ t^{m+1}).$$

It is clear that $M_m(k, b) = k! N_m(k, b)$. We are interested in when $M_m(k, b) > 0$ and when there is a good asymptotic formula.

Let $A = \mathbf{F}_q[t]/(t^{m+1})$ be the residue class ring. Let A^* be the set of all the invertible elements of A. A multiplicative character $\chi : A^* \to \mathbb{C}^*$ is a homomorphism from A^* to the non-zero complex numbers $\mathbb{C}^*$. Let $\widehat{A^*}$ be the group of multiplicative characters of A^*. Let $G = \{\chi \in \widehat{A^*}, \chi(\mathbf{F}_q^*) = 1\}$. Note that G is an abelian group of order q^m. Let $X = \mathbf{F}_q^k$. Let

$$\overline{X} = \{(x_1, x_2, \ldots, x_k) \in \mathbf{F}_q^k | x_i \neq x_j,\ \forall\, i \neq j\}.$$

It is clear that $|X| = q^k$ and $|\overline{X}| = (q)_k$. Similarly, for a permutation $\tau \in S_k$, X_τ consists of the elements $x \in X$ of type τ. By definition, we have

$$\begin{aligned} M_m(k, b) &= \frac{1}{q^m} \sum_{x \in \overline{X}} \sum_{\chi \in G} \chi\left(\frac{(1 + x_1 t)(1 + x_2 t) \cdots (1 + x_k t)}{1 + b_1 t + \cdots + b_m t^m} \right) \\ &= \frac{1}{q^m} \sum_{x \in \overline{X}} \sum_{\chi \in G} \chi^{-1}(1 + b_1 t + \cdots + b_m t^m) \chi\left(\prod_{i=1}^{k} (1 + x_i t) \right), \end{aligned}$$

For given $\chi \in G$, let

$$f_\chi(x) = f_\chi(x_1, x_2, \ldots, x_k) = \chi\left(\prod_{i=1}^{k} (1 + x_i t) \right).$$

Let $b(t) = 1 + b_1 t + \cdots + b_m t^m$. Then, we can rewrite

$$q^m M_m(k, b) = \sum_{\chi \in G} \chi^{-1}(b(t)) \sum_{x \in \overline{X}} f_\chi(x_1, x_2, \ldots, x_k).$$

Obviously X is symmetric. It is also easy to check that $f_\chi(x_1, x_2, \ldots, x_k)$ is normal on X. Thus by applying Proposition 2.8, we deduce

$$q^m M_m(k, b) = \sum_{\chi \in G} \chi^{-1}(b(t)) \sum_{\tau \in C_k} \mathrm{sign}(\tau) C(\tau) F_\tau(\chi) = (q)_k + \sum_{\chi \neq 1} \chi^{-1}(b(t)) \sum_{\tau \in C_k} \mathrm{sign}(\tau) C(\tau) F_\tau(\chi),$$

where C_k is the set of conjugacy classes of S_k, $C(\tau)$ is the number of permutations conjugate to τ, and

$$F_\tau(\chi) = \sum_{x \in X_\tau} \prod_{i=1}^{k} \chi(1 + x_i t).$$

For a non-trivial character $\chi \in G$, since $\chi(\mathbf{F}_q^*) = 1$, the Weil bound (26) gives

$$\left|1+\sum_{a\in\mathbf{F}_q}\chi(a+t)\right|\leqslant(m-1)\sqrt{q}.$$

This and the fact that $\chi(t)=0$ implies

$$\left|\sum_{a\in\mathbf{F}_q}\chi(1+at)\right|\leqslant(m-1)\sqrt{q}$$

and thus

$$\left|\sum_{x\in X}\prod_{i=1}^{k}\chi(1+x_it)\right|\leqslant((m-1)\sqrt{q})^k.$$

For given $\tau\in C_k$, assume τ is of type $(c_1,c_2,\ldots,c_k)$, where c_i is the number of i-cycles in τ for $1\leqslant i\leqslant k$. Note that $\sum_{i=1}^k ic_i=k$ and thus we deduce

$$\begin{aligned}F_\tau(\chi)&=\Big(\sum_{a\in\mathbf{F}_q}\chi(1+at)\Big)^{c_1}\Big(\sum_{a\in\mathbf{F}_q}\chi^2(1+at)\Big)^{c_2}\cdots\Big(\sum_{a\in\mathbf{F}_q}\chi^k(1+at)\Big)^{c_k}\\&=\prod_{i=1}^{k}\Big(\sum_{a\in\mathbf{F}_q}\chi^i(1+at)\Big)^{c_i}\leqslant q^{\sum_{i=1}^k c_im_i(\chi)}((m-1)\sqrt{q})^{\sum_{i=1}^k c_i(1-m_i(\chi))},\end{aligned}\tag{27}$$

where $m_i(\chi)$ is defined as follows: $m_i(\chi)=1$ if $\chi^i=1$ and $m_i(\chi)=0$ if $\chi^i\neq1$. Thus

$$\begin{aligned}q^mM_m(k,b)&=(q)_k+\sum_{\chi\neq1}\chi^{-1}(b(t))\sum_{\tau\in C_k}\operatorname{sign}(\tau)C(\tau)F_\tau(\chi)\\&=(q)_k+\sum_{\chi^d\neq1,\forall2\leqslant d\leqslant k}\chi^{-1}(b(t))\sum_{\tau\in C_k}\operatorname{sign}(\tau)C(\tau)F_\tau(\chi)\\&\quad+\sum_{\chi\neq1,\chi^d=1,\text{ for some }2\leqslant d\leqslant k}\chi^{-1}(b(t))\sum_{\tau\in C_k}\operatorname{sign}(\tau)C(\tau)F_\tau(\chi).\end{aligned}$$

Let τ be a permutation of type $(c_1,c_2,\ldots,c_k)$. Since in the first summation we always have $\chi^d\neq1$ for every d with $1\leqslant d\leqslant k$, thus $m_i(\chi)=0$ for any such χ and any i with $1\leqslant i\leqslant k$. By (27) we conclude that

$$F_\tau(\chi)\leqslant((m-1)\sqrt{q})^{c_1+c_2+\cdots+c_k}.$$

Let $S=\sharp\{\chi\in G|\chi^d=1,\text{for some }2\leqslant d\leqslant k\}$. Then, by the enumeration formula for $C(\tau)$ given by (17) we have

$$\begin{aligned}|q^mM_m(k,b)-(q)_k|&\leqslant\sum_{\chi^d\neq1,\forall2\leqslant d\leqslant k}\sum_{\tau\in C_k}C(\tau)|F_\tau(\chi)|+\sum_{d=2}^{k}\sum_{\chi^d=1,\chi^{d'}\neq1\text{ for }d'<d}\sum_{\tau\in C_k}C(\tau)|F_\tau(\chi)|\\&\leqslant(q^m-S)\sum_{\sum ic_i=k}\frac{k!}{1^{c_1}c_1!2^{c_2}c_2!\cdots k^{c_k}c_k!}((m-1)\sqrt{q})^{\sum_{i=1}^k c_i}\\&\quad+S\cdot\sum_{\sum ic_i=k}\frac{k!}{1^{c_1}c_1!2^{c_2}c_2!\cdots k^{c_k}c_k!}q^{\sum_{i=1}^k c_im_i(\chi)}((m-1)\sqrt{q})^{\sum_{i=1}^k c_i(1-m_i(\chi))}.\end{aligned}$$

Note that the χ in the last summation is a d-th primitive character, that is, $m_i(\chi)=1$ if and only if $d|i$. Thus it follows from (21), (22) and Corollary 4 that

$$|q^mM_m(k,b)-(q)_k|\leqslant(q^m-S)((m-1)\sqrt{q}+k-1)_k+S\max_d\left(\frac{q+(d-1)(m-1)\sqrt{q}}{d}+k-1\right)_k,$$

where d runs over the non-trivial divisors of $|G|=q^n$. In particular, $d\geqslant p$. Thus

$$\begin{aligned}|q^mM_m(k,b)-(q)_k|&\leqslant(q^m-S)((m-1)\sqrt{q}+k-1)_k+S\cdot(q/p+(m-1)\sqrt{q}+k-1)_k\\&<q^m(q/p+(m-1)\sqrt{q}+k-1)_k.\end{aligned}$$

It follows that we have

Theorem 5.2.

$$\left|N_m(k,b)-\frac{1}{q^m}\binom{q}{k}\right|<\binom{q/p+(m-1)\sqrt{q}+k-1}{k}.$$

Theorem 5.3. *For any $\epsilon>0$, there is a constant $c_\epsilon>0$ such that if $m<\epsilon k^{1/2}$ and $4\epsilon^2\ln^2 q<k\leqslant c_\epsilon q$, then $N_m(k,b)>0$ for all $b\in\mathbf{F}_q^m$.*

Proof. By Theorem 5.2, it is sufficient to prove

$$\frac{1}{q^m}\binom{q}{k}\geqslant\binom{q/p+m\sqrt{q}+k}{k},$$

that is,

$$\frac{(q)_k}{(q/p+m\sqrt{q}+k)_k}\geqslant q^m.$$

This leads to the following inequality:

$$\frac{q}{q/p+m\sqrt{q}+k}\geqslant q^{m/k}.$$

For any $\epsilon>0$, assume $m<\epsilon k^{1/2}$ and $k\leqslant cq$, we then have

$$\frac{q}{q/p+m\sqrt{q}+k}\geqslant\frac{q}{q/p+\epsilon c^{1/2}q+qc}\geqslant q^{m/k}.$$

Thus if the constant c satisfies the inequality $\epsilon c^{1/2}+c\leqslant\frac{1}{q^{m/k}}-\frac{1}{p}$, then for any $k\leqslant cq$, we have $N_m(k,b)>0$. This is possible if $q^{m/k}<\sqrt{e}$ for the natural number $e>1$, that is, if $\frac{m}{k}<\frac{\epsilon}{\sqrt{k}}<\frac{1}{2\ln q}$. This last inequality is satisfied if we take $k>4\epsilon^2\ln^2 q$. The proof is complete. □

Acknowledgements This paper was written when the second author was visiting the Institute of Mathematics at the Chinese Academy of Sciences and the Center for Advanced Study at Tsinghua University. The second author would like to thank both institutions for their hospitality. The first author was supported in partial by Science and Technology Commission of Shanghai Municipality(Grant No. 09XD1402500). The second author was partially supported by NSF.

References

1 Cheng Q, Murray E. On deciding deep holes of Reed-Solomon codes. In: TAMC 2007, Lecture Notes in Computer Science, vol. 4484. Berlin-Heidelberg: Springer, 2007
2 Cheng Q, Wan D. On the list and bounded distance decodibility of Reed-Solomon codes. In: FOCS (2004). 45th Annual IEEE Symposium on Foundation of Computer Science. Rome: IEEE Computer Society Press, 2004, 335–341
3 Cheng Q, Wan D. On the list and bounded distance decodability of Reed-Solomon codes. SIAM J Comput, 2007, 37: 195–209
4 Cheng Q, Wan D. Complexity of decoding positive-rate Reed-Solomon codes. In: Proceedings of ICALP08, Lecture Notes in Computer Sciences, vol. 5125. Berlin-Heidelberg: Springer, 2008, 283–293
5 Cheng Q, Wan D. A deterministic reduction for the gap minimun distance problem. In: STOC 2009, 41st ACM Symposium on Theory of Computing. New York: ACM Press, 2009, 33–38
6 Chung F. Diameters and eigenvalues. J Amer Math Soc, 1989, 2: 187–196
7 Cohen S D. Polynomial factorization and an application to regular directed graphs. Finite Fields Appl, 1998, 4: 316–346
8 Katz N. Facoring polynomials in finite fields: an application of Lang-Weil to a problem in graph theory. Math Ann, 1990, 286: 625–637
9 Li J Y, Wan D. On the subset sum problem over finite fields. Finite Fields Appl, 2008, 14: 911–929
10 Li Y J, Wan D. On error distance of Reed-Solomon codes. Sci China Ser A, 2008, 51: 1982–1988
11 Stanley R P. Enumerative Combinatorics, vol. 1. Cambridge: Cambridge University Press, 1997
12 Wan D. Generators and irreducible polynomials over finite fields. Math Comp, 1997, 66: 1195–1212
13 Wang Y. Wang Yuan Selected Papers (in Chinese). Changsha: Hunan Education Press, 1999