Generalization of GCD matrices

Haiqing Han1 · Qin Li2 · Yi Wen1 · Shuang Wen1 · Jie Li1

Received: 11 November 2019 / Revised: 7 June 2020 / Accepted: 27 September 2020 / Published online: 16 October 2020

© Springer-Verlag GmbH Germany, part of Springer Nature 2020

Abstract
Special matrices are widely used in information society. The gcd-matrices have been conducted to study over Descartes direct-product of some finite positive integer sets. If Descartes direct-product $S = S_1 \times S_2 \times \cdots \times S_n$ with $n$ finite positive integer sets as direct product terms, then $S$ is finite too. Without loss of generality, set $S = \{d_1, d_2, \ldots, d_t\}$, and $\forall a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n) \in S$, the general greatest common factor is defined as $\gcd(a, b) = \prod_{i=1}^{n} \gcd(a_i, b_i)$. And create a square matrix $(S) = (s_{ij})_{n \times n}$ possessed the general greatest common factors $\gcd(d_i, d_j)$ as arrays $s_{ij} = \gcd(d_i, d_j)$. We have researched upper bound and lower bound of the determinant $\det(S)$ of the $t \times t$ gcd-matrix $(S)$, and compute the determinant’s value under special or specific conditions in the article. At last, some well results about the gcd-matrix has been extend from Descartes direct-product of some finite positive integer sets to general direct product of the posets.

Keywords Greatest common divisor matrix · Descartes direct-product · Meet semilattice · Meet matrices · Generalized Euler’s $\phi$-function · Mobius inversion

1 Introduction
The gcd-matrix $(S)$ standing for the greatest common divisor matrix is a special type of matrix that the arrays come from a positive integers set $S = \{a_1, a_2, \ldots, a_n\}$. The nature of its determinants $\det(S)$ has increasingly become a hot topic of scientific research in many application fields. The authors such as S. Beslin, S. Ligh etc. have taken the lead in giving a definition of the greatest common factor matrix [4, 18, 19, 22, 23] (that is gcd-matrix $(S)$) over the finite natural number set $S = \{a_1, a_2, \ldots, a_n\}$. Set the square matrix $(S) = (s_{ij})_{n \times n}$ with the arrays $s_{ij} = \gcd(a_i, a_j)$, the array $s_{ij} = \gcd(a_i, a_j)$ is the greatest common factor between $a_i$ and $a_j$. The greatest common factor (or greatest common divisor) is abbreviated to GCD. And that naturally gives rise to the concept of a gcd-matrix $(S)$. Z. Li has pointed out $\det(S) = \phi(a_1)\phi(a_2) \cdots \phi(a_n)$ in [14, 26], where $S$ is the FC set and $\phi$ is the Euler’s totient function. While the set is said a FC set, if all positive integer factors of $a \in S$ are contained in the set $S$. Namely, if $\forall a \in S$ and $d \mid a$ then $d \in S$. The matrix $(S)_{\phi} = (s_{ij})_{n \times n}$, $s_{ij} = g((a_i, a_j))$ $(i, j = 1, 2, \ldots, n)$ and $g((a_i, a_j))$ refers to the value of the arithmetic function $g$ on the greatest common factor $\gcd(a_i, a_j)$ [1, 2, 7, 8, 12, 13, 21]. The following conclusions are proved by H.J.S. Smith [7]: if the set $S$ is hypothetical to FC, then completely satisfactory formula $\det(S)_{\phi} = (g \odot \mu)(a_1)(g \odot \mu)(a_2) \cdots (g \odot \mu)(a_n)$ holds, where $g \odot \mu$ just happens to be the convolution between $g$ and the mobius function $\mu$. The conclusions in [7, 26] have been extended respectively the corresponding promotion, and they have obtained some good results [5, 10, 11]. This article has obtained some new promotion to the gcd-matrix based on the key outcomes in [17, 24, 25]. These properties are widely used in the communication theory, the algebraic coding theory, the cryptography and other fields [3, 9, 15]. For the convenience of introduction, the following definitions have been given first.

Definition 1 [25] Let $U$ be a poset, $p$ be its partial order. Called $U$ the meet semilattice, when $\forall a, b \in U$, there exists the unique element $\omega \in U$. The element $\omega$ satisfies: (i) $\omega \leq a$
and \( apb \); (ii) there exists \( z \in U \) so that \( zpx \) and \( zpy \), it does deduce \( zpa \).

Where \( \omega \) is known as the meet confirmed by a and b, and the notation indicates \( \omega = (a, b)_p \).

**Definition 2** Set \( S = \{ a_1, a_2, \ldots, a_n \} \) a subset owned by \( U \) a meet semilattice, the subset \( S \) satisfied the MC (meet closed) condition, that is \( \forall a, b \in S \) iff \( (a, b)_p \in S \), at the same time, \( S \) is named as the meet closed set (namely MCS). In the same way, that \( S \) named as low closed set, for all \( a \in S, b \in U \) and \( bpa \), iff \( b \in S \), then the low closed set \( S \) has been abbreviated to “the LCS”. LC set must satisfy MC set, but not vice versa. The “LCS and MCS” are respectively the corresponding extension to the conception “FC set and GCDC set”.

**Definition 3** [25] Set \( S = \{ a_1, a_2, \ldots, a_n \} \) a finite subset included in the meet semilattice \( U \), h is a mapping defined on \( U \), that is \( h : U \to R \), the function value \( R \) is an abelian ring with the unit element, it expressed \( \langle S \rangle_h = (s_i)_{i=1}^n \), \( s_i = h(a_i, a_j)(i, j = 1, 2, \ldots, n) \). The matrix \( \langle S \rangle_h \) is known as a meet-matrix about the function \( h \) over the poset \( S \). Its shorter form is the meet matrix. Generally speaking, the abelian ring \( R \) is the all real number set.

So the meet matrix on the poset \( S \) is as below

\[
\begin{pmatrix}
(\langle a_1, a_j \rangle_h) \\
(\langle a_2, a_j \rangle_h) \\
(\langle a_n, a_j \rangle_h)
\end{pmatrix}
\]

**Definition 4** Set \( S = \{ x_1, x_2, \ldots, x_n \} \) a partial order subset included in meet semi-lattice \((U, p)\), the function by recursive definition \( \Psi_{S,x}(x_i) = g(x_i) - \sum_{x_p \in S, x \neq x_j} \Psi_{S,x}(x_j) \), its take the value 0 when the subscript sum item is null set. Set \( g \) is the real function denoted by \( g : U \to R \). \( \Psi_{S,x} \) be known as the generalized euler’s \( \Psi \)-function on the partial order subset \( S \).

**Remark 1** It is easy to know from definition 4, the backstepping formula \( g(x_i) = \sum_{x_p \in S} \Psi_{S,x}(x_j) \) sets up when \( S \) is a partial order subset of the meet semi-lattice \( U \), then the function \( \Psi_{S,x}(x_i) = \sum f(x_i)\mu(x_i, x) \) come from the mobius inversion [20], and \( \mu \) is the mobius function on the partial order subset \( S \) with the partly ordered relation \( p \).

As previously defined, the concept of the gcd-matrix has been generalized onto the Descartes direct product. There are \( n \) positive integer finite sets \( S_1, S_2, \ldots, S_n \), for all \( 1 \leq i \leq n \), there exists the partly ordered relation \( p_i \), belonged to the partial order subset \( S_i \), namely \( \forall a_i, b_i \in S_i, a_i p_i b_i \), if and only if \( a_i b_i \) denoted by the divisible relation of natural numbers. So \( (S, p) \) be the partial order set. Using Definition 1, the natural number set \( N \) can become a meet semi-lattice under the condition of the partly ordered relation is divisibility relation. Moreover, the meet of any two natural numbers is the greatest common divisor. So \( (S, p) \) is viewed as a subset that can be embedded in some meet semilattice. We have the result: if \( \forall a_i, b_i \in S_i \), then \( (a_i, b_i) = \gcd(a_i, b_i) \).

And set \( S = S_1 \times S_2 \times \cdots \times S_n \) defined a divisibility relation as the partially ordered \( p \) on the natural number set \( S \). For all \( \forall a_i = (a_{i1}, a_{i2}, \ldots, a_{in}), b_i = (b_{i1}, b_{i2}, \ldots, b_{in}) \in S \), make \( a p b \Leftrightarrow (a_i p_i (i = 1, 2, \ldots, n)) \). Still is denoted by \( (S, p) \) a poset. Every set \( S_i \) is finite set, so is \( S \). Without loss of generality, let \( S = \{ d_1, d_2, \ldots, d_q \} \), where the enumeration \( q = |S_1| \times |S_2| \times \cdots \times |S_n| \), \( |S_i| \) denotes the cardinality of the set \( S_i \). At the same time, \( \forall a_i, b_i \in S \), we have two points as follows:

(i) if \( a b \Leftrightarrow ab \), a is called one factor of \( b \).

(ii) \( gcd(a, b) = \prod_{i=1}^{n} gcd(a_i, b_i) \), where \( \forall a_i = (a_{i1}, a_{i2}, \ldots, a_{in}) \), \( b_i = (b_{i1}, b_{i2}, \ldots, b_{in}) \in S_i \).

So \( (S, p) \) viewed as a subset can be embedded in some meet semilattice denoted by \( N \times N \times \cdots \times N \), fulfilled

\[
(a, b)_p = ((a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n))
\]

The \( q \times q \) meet-matrix over \( S \) is defined as \( \langle S \rangle = (gcd(d_i, d_j))_{q \times q} \). In order to vivid charm, \( \langle S \rangle \) is still known as the gcd-matrix. Investigators have found out that the gcd-matrix and generalized Euler’s \( \Psi \)-function have close relationships.

Let \( \Psi_{S,x} \) be the broad sense Euler’s totient function over the set \( S \), take \( f(d_j) = d_j^{(1)} \times d_j^{(2)} \times \cdots \times d_j^{(n)} \) \( \forall d_j \in S \). We have defined a generalized Euler’s \( \Psi_{S,x} \)-function over the set \( S \) as follows: \( \Psi_{S,x}(d_j) = f(d_j) - \sum_{d_{i1} \neq d_j} \Psi_{S,x}(d_{i1}) \) where \( f(d_j) = d_j^{(1)} \times d_j^{(2)} \times \cdots \times d_j^{(n)} \) note the product of the component in \( d_j \). Now, we can study the gcd-matrix on \( S = S_1 \times S_2 \times \cdots \times S_n \) \( = \{ d_1, d_2, \ldots, d_q \} \). Suppose \( \forall d_i \in S = S_1 \times S_2 \times \cdots \times S_n \), \( d_i = (d_{i1}, d_{i2}, \ldots, d_{in}) \) is a n-dimensional vector. We have gotten a gcd-matrix over \( S = S_1 \times S_2 \times \cdots \times S_n \) \( = \{ d_1, d_2, \ldots, d_q \} \) as follows:

\[
\langle S \rangle_{q \times q} = \begin{pmatrix}
(d_1, d_1)_p & (d_1, d_2)_p & \cdots & (d_1, d_q)_p \\
(d_2, d_1)_p & (d_2, d_2)_p & \cdots & (d_2, d_q)_p \\
\vdots & \vdots & \ddots & \vdots \\
(d_q, d_1)_p & (d_q, d_2)_p & \cdots & (d_q, d_q)_p
\end{pmatrix}
\]

\[
= \begin{pmatrix}
\prod_{k=1}^{n} (d_1^{(k)}, d_1^{(k)})_p & \prod_{k=1}^{n} (d_1^{(k)}, d_2^{(k)})_p & \cdots & \prod_{k=1}^{n} (d_1^{(k)}, d_q^{(k)})_p \\
\prod_{k=1}^{n} (d_2^{(k)}, d_1^{(k)})_p & \prod_{k=1}^{n} (d_2^{(k)}, d_2^{(k)})_p & \cdots & \prod_{k=1}^{n} (d_2^{(k)}, d_q^{(k)})_p \\
\vdots & \vdots & \ddots & \vdots \\
\prod_{k=1}^{n} (d_q^{(k)}, d_1^{(k)})_p & \prod_{k=1}^{n} (d_q^{(k)}, d_2^{(k)})_p & \cdots & \prod_{k=1}^{n} (d_q^{(k)}, d_q^{(k)})_p
\end{pmatrix}
\]
where \((d_i, d_j)_p = gcd(d_i, d_j) = \prod_{k=1}^{n} (d_i^{(k)}, d_j^{(k)})_{p_k} = \prod_{k=1}^{n} gcd(d_i^{(k)}, d_j^{(k)})\).

After we have obtained the gcd-matrix on \(S = S_1 \times S_2 \times \cdots \times S_n = \{d_1, d_2, \ldots, d_q\}\), the nature of the gcd-matrix have been researched in next section. In this paper, we have two generalizations: first, we extend the GCD matrix to the Descartes direct-product of some finite positive integer sets and the general direct product of the posets; second, we define the generalized Euler’s totient-function. And the relation between the determinant of the generalized GCD matrix and the generalized Euler’s totient-function is studied.

2 Main results

Next, we have studied the generalized gcd-matrix (or called meet matrix) over \(S = S_1 \times S_2 \times \cdots \times S_n\) used the Mobius inversion. Set \(T_1, T_2, \ldots, T_n\) finite natural number sets, \(T_i (i = 1, 2, \ldots, n)\) denote a minimum GCDC set containing the set \(S_i\) (where the smallest GCDC set refers to be contained in the intersection of all GCDC subsets of \(S_i\)). As previously mentioned, \(T_i\) is a poset under the divisibility relation. Still the partially ordered relation of \(T_i\) denotes by \(\rho\) (\(\rho\) is actually divisibility relation). So \(\Psi_T\) is the generalized Euler’s \(\Psi\)-function on \(T_i\), \(\Psi_T = \{f_1, f_2, \ldots, f_i\}\), it must satisfy \(T \supseteq S_i\), and \(T\) is MCS by Definition 4. For the structure of the generalized gcd-matrix on \(S = S_1 \times S_2 \times \cdots \times S_n\).

We have drawn the following conclusions to the generalized Euler’s totient function:

**Theorem 1** Set \(S = S_1 \times S_2 \times \cdots \times S_n = \{d_1, d_2, \ldots, d_q\}\) and \(T = T_1 \times T_2 \times \cdots \times T_n = \{f_1, f_2, \ldots, f_t\}\), then \((S) = AA^T = EAET^T\), so \((S)\) is the positive definite. Where \(A = (a_{ij})_{n \times n}, A = diag(\Psi_T(f_1), \Psi_T(f_2), \ldots, \Psi_T(f_t))\). The matrices \(A^T\) and \(E^T\) are respectively the transpose matrices to \(A\) and \(E\), \(\Psi_T\) is the generalized Euler’s totient function on \(T\). And 

\[e_y = \begin{cases} 1 & f_{p'd_{i'}} \, \text{if } a_{ij} = 1, e_y(\Psi_T(f_j))^{1/2}. \\ 0 & \text{otherwise} \end{cases}\]

According to this theorem, we can calculate the determinant of \((S)\), and have the following theorem:

**Theorem 2** Set \(S = S_1 \times S_2 \times \cdots \times S_n\) and \(T = T_1 \times T_2 \times \cdots \times T_n\), are all Descartes direct product of \(n\) sets, so the determinant is expanded as follows:

\[
\det (S) = \sum_{1 \leq k_1 < k_2 < \cdots < k_n \leq S} \left[ \det E(k_1, k_2, \ldots, k_n) \right]^2 \Psi_T(f_{k_1}) \Psi_T(f_{k_2}) \cdots \Psi_T(f_{k_n}).
\]

where \(E = (e_{ij})_{n \times n}\) is the \(0 \times 1\) matrix \(e_{ij}\) is 

\[e_{ij} = \begin{cases} 1 & f_{p'd_{i'}} \, \text{if } a_{ij} = 1, e_y(\Psi_T(f_j))^{1/2}. \\ 0 & \text{otherwise} \end{cases}\]

the sub-matrix \(E(k_1, k_2, \ldots, k_n)\) has been formed by taking out \(k_1\)th, \(k_2\)th, \ldots, \(k_n\)th columns of the \(0 \times 1\) matrix \(E\) and retaining the initial corresponding position unchanged. By the following Theorem 3, We can have a discussion on upper-lower bounds of the meet-matrix’s determinant, it is expressed the following theorem.

**Theorem 3** Set \(S = S_1 \times S_2 \times \cdots \times S_n\), \(T = T_1 \times T_2 \times \cdots \times T_n\), so the following 3 conclusions are established:

(i) (determinant’s lower bound) \(\det (S) \geq \prod_{d \in S} \Psi_T(d)\), its equality is true if the set \(S\) is MCF, and the factor of any one element in \(S\) does not exist in the difference set \(T\);

(ii) (the determinant’s upper bound) \(\det (S) \leq \prod_{d \in T} (d^{(1)} \times d^{(2)} \times \cdots \times d^{(n)});

(iii) (equality) If each \(S_i\) be FC set, then \(\det (S) = \prod_{\{a \in S\} \in S} \phi(x_1) \phi(x_2) \cdots \phi(x_n)\) where \(\phi\) is the Euler’s totient function.

It is a special case of the third item in the Theorem 3. We have a certain understanding to the greatest common divisor matrix on \(S = S_1 \times S_2 \times \cdots \times S_n\), especially the structure and its determinants of the matrices.

3 Proofs of the above 3 theorems

Starting from this part, the authors have priority task to prove the 3 theorems mentioned above, it is to need the following proposition:

**Proposition 1** Let the set \(S = \{a_1, a_2, \ldots, a_n\}\) be partial order, and \(p\) be the partially ordered relation, then \(S\) may be orderly arranged \(a_1, a_2, \ldots, a_n\), and if \(a_i < a_j\) then \(i < j\).

**Proposition 2** Let the finite set \(S = \{a_1, a_2, \ldots, a_n\}\) be GCD, the set \(T = \{y_1, y_2, \ldots, y_n\}\) included the set \(S\) be FC, if \(a_1 < a_2 < \cdots < a_n\), then \(\Psi_T(a_i) = \sum_{\{\phi(z)\} \in S} \phi(z), \forall j \geq 1\), where the subscript set \(V_a = \{z \in T : \min\{y \in S : z \mid y\} = a_j\}\) and take as \(a_0 = 0\).

**Remark** The proposition has indicated that if the natural number set \(S = \{a_1, a_2, \ldots, a_n\}\) is GCD, then the broad sense Euler’s totient \(\Psi\)-function \(\Psi_S(a) \geq \phi(a), \forall a \in S\), where \(\phi\) is the Euler’s function. When the set \(S\) is FC, so \(\Psi_S(a) = \phi(a), \forall a \in S\), because of \(S = T\) and \(d\)
definite, and the $n \times n$ matrix $D$ is positive semi-definite, then the determinant satisfies $\det(C + D) \geq \det C + \det D$, when the equality establishes if the order $n \geq 1$ and $D$ is a zero matrix.

**Proposition 4** [20] Let $\mu_\omega$ be the Mobius function on the locally finite poset $\Omega$, then

(i) When $\rho$ is an isomorphic mapping from the poset $\Omega$ to $P$, $\mu_\omega(\rho(a), \rho(b)) = \mu_\omega(a, b) \in \Omega$.

(ii) $\mu_\omega(a, b) = \prod_{j=1}^k \mu_\omega(\eta_j, \eta_j')$ in the direct product of the poset $\Omega = \Omega_1 \times \Omega_2 \times \cdots \times \Omega_k$, where $\forall a = (a_1, a_2, \ldots, a_k), b = (b_1, b_2, \ldots, b_k) \in \Omega$.

In addition, we have given two following lemmas.

**Lemma 1** If Descartes direct product $S = S_1 \times S_2 \times \cdots \times S_n$, $\forall a = (a_1, a_2, \ldots, a_n) \in S$, then the general Euler's totient $\Psi_S$ -function: $\Psi_S(x) = \prod_{i=1}^k \Psi_S(x_i)$.

**Proof** Let $S = \{d_1, d_2, \ldots, d_q\}$ be Descartes direct product, and the Euler's totient $\Psi_S$ -function over $S$ is generalized, we know as the product $d^{(1)}_1 \times d^{(2)}_1 \times \cdots \times d^{(n)}_1 = \prod_{d_i \in P_1}^n \Psi_S(d_i)$. In order to profile, $\forall d_1 \in S$ written the product $|d| = d^{(1)}_1 \times d^{(2)}_1 \times \cdots \times d^{(n)}_1$. By Remark 1, we have $\Psi_S(d) = \sum_{d_i \in P_1}^n \Psi_S(d_i, d_j)$. From the Proposition 3,

$$\Psi_S(d) = \prod_{\ell=1}^n \left( \sum_{d_{i_1} \in \omega_1}^n \cdot \sum_{d_{i_2} \in \omega_2}^n \cdots \sum_{d_{i_n} \in \omega_n}^n \Psi_S(d^{(i_1)}_1, d^{(i_2)}_2, \ldots, d^{(i_n)}_n) \right)$$

Just exchange between $d_j$ and $x$, so the lemma holds. □

**Lemma 2** [16] Let the real matrix $A$ be positive definite, if $A_{mn} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ then $\det A \leq a_{11}a_{22} \cdots a_{nn}$.

Now, our main results are proved as follows:

**The proof process of Theorem 1** Take $A = \text{diag}(\Psi_T(f_1), \Psi_T(f_2), \ldots, \Psi_T(f_j))$, then $D = EA = (e_i \Psi_T(f_j))_{i \leq j}$. So the $(i, j)$ -array in $E\text{AE}^T$ is

$$\sum_k e_{ik} \Psi_T(f_k) e_{jk} = \sum_{f_i \in d_i} \Psi_T(f_i) = \sum_{f_i \in d_i} \Psi_T(f_i) = \sum_{f_i \in \text{gcd}(d_i)} \Psi_T(f_i)$$

Hence we have gained $<S > = E\text{AE}^T$. From Lemma 1, it comes very naturally to get the formula $\Psi_S(a) = \prod_{\ell=1}^n \Psi_S(a_{\ell})$. From proposition 2, the set $T_k(k = 1, 2, \ldots, n)$ is GCD, when the function satisfies $\Psi_T(f) \geq \phi(y_k) > 0$, so the Euler's function satisfies $\Psi_T(f) = 0$. Suppose $A = EA_{1/2} = \text{diag}(\sqrt{\Psi_T(f_1)}, \sqrt{\Psi_T(f_2)}, \ldots, \sqrt{\Psi_T(f_j)})$, then $\sqrt{S} = A_{\text{AE}^T}$, that is to say $<S > = A_{\text{AE}^T} = E\text{AE}^T$. So perfect is to the Theorem 1. The proof process of Theorem 2 is as follows:

**Proof of Theorem 2** It is easy from the proof process of Theorem 1 to know the following results $<S > = E\text{AE}^T$. Take the matrix $D = EA = (e_i \Psi_T(f_j))_{i \leq j}$. By the Cauchy-Binet formula [6] to decompose matrix $<S > = E\text{AE}^T$.

$$\det(S) = \det(\text{DE}^T)$$

$$= \sum_{1 \leq i < k < \cdots < k_q} \det(D(k_1, k_2, \ldots, k_q) \times \text{DE}^T(k_1, k_2, \ldots, k_q)$$

$$= \sum_{1 \leq i < k < \cdots < k_q} \text{DE}^T(k_1, k_2, \ldots, k_q)$$

The third equation is established because each column extracts the common factor in the following determinant $D$.

$$\det D = \begin{vmatrix} e_{1k_1} \Psi_T(f_{k_1}) & e_{1k_2} \Psi_T(f_{k_2}) & \cdots & e_{1k_q} \Psi_T(f_{k_q}) \\ e_{2k_1} \Psi_T(f_{k_1}) & e_{2k_2} \Psi_T(f_{k_2}) & \cdots & e_{2k_q} \Psi_T(f_{k_q}) \\ \vdots & \vdots & \ddots & \vdots \\ e_{qk_1} \Psi_T(f_{k_1}) & e_{qk_2} \Psi_T(f_{k_2}) & \cdots & e_{qk_q} \Psi_T(f_{k_q}) \end{vmatrix}$$

Thereupon then the Theorem 2 is correct. □

**Corollary 1** If the set $S = S_1 \times S_2 \times \cdots \times S_n$ is MC, then the determinant $\det[S] = \prod_{i=1}^n \Psi_S(d_i)$.

**Proof** By Proposition 1, we have known that if $d_{i \neq j}$ and $d_i \neq d_j \Rightarrow i < j$ to $S$. By Theorem 2, the matrix $E = (e_{ij})$ is the lower triangular matrix that the main diagonal are all 1. That is if $i < j$ then $e_{ij} = 0$ and $e_{ii} = 1$. The lower triangular matrix is

$$E = (e_{ij}) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ e_{21} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ e_{n1} & e_{n2} & \cdots & 1 \end{pmatrix}$$

So is correct to the conclusion. □
The proof process to Theorem 3 It is easy from Theorem 2 to know that $S > = EAE^T$ and $A = diag(\Psi_T(f_1), \Psi_T(f_2), \ldots, \Psi_T(f_i))$. By Lemma 2, $\forall y = (y_1, y_2, \ldots, y_n) \in T$, $\Psi_T(y) = \prod_{k=1}^n \Psi_T(y_k)$. Because $T_k$ is the $k$-th GCDC set, so $\Psi_T(y) \geq \phi(y) > 0$, namely $\Psi_T(y) > 0$ by Proposition 1. Thus the matrix $\langle S \rangle$ is positive-definite matrix.

According to the Theorem 2, the inequality holds.

$$\det \langle S \rangle = \prod_{i=1}^q \text{gcd}(d_i, d_i) \geq \prod_{i=1}^q (d_i^{(1)} \times d_i^{(2)} \times \cdots \times d_i^{(n)})$$

(iii) If the poset $S$ is FC, then the two sets are equal, namely $S = T$. We have known $\Psi_T(y_k) = \phi(y_k)$ by Remark 2, therefore, $\Psi_T(y) = \prod_{k=1}^n \Psi_T(y_k) = \prod_{k=1}^n \phi(y_k)$. So

$$\det \langle S \rangle = \prod_{d \in S} \Psi_T(d) = \prod_{d \in S} \phi(d) = \prod_{d \in S} \phi(d)$$

Where $\phi$ is the Euler’s totient $\phi$-function. To make a long story short, the conclusions (i) (ii) (iii) are all hold, and the proof of Theorem 4 have been finished now.

Remark 2 It is clearly to the above process for $S = S_1 \times S_2 \times \cdots \times S_n$ that, if $n = 1$, then it can get the content discussed in [7]; if $n = 2$ that is $S = S_1 \times S_2$, then $\langle S \rangle = \langle S_1 \rangle \otimes \langle S_2 \rangle$, where $\otimes$ is the tensor product.

4 The generalization of gcd matrix on a general poset

Many properties of gcd-matrices are related to the ordered relations of set, we can study generalized gcd-matrix on the general partial order set. In order to discuss more properties of the gcd-matrix and meet matrix, we have studied the meet matrix from the direct product of a general poset.

Set the $n$ sets $P_1, P_2, \ldots, P_n$ are all meet semi-lattices, naturally occurring respective partialy ordered relation. The notation $p_i = (i, 1, 2, \ldots, n)$ is expressed the corresponding partial order relation of $P_i$, then $P = P_1 \times P_2 \times \cdots \times P_n$ is also a poset and the meet semi-lattice with the partial order relation $p$. $\forall a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n) \in P$, $a \wedge b = a_i b_i, (i = 1, 2, \ldots, n)$.

Then the meet between $x$ and $y$ is

$$(a, b)_p = ((a_1, b_1)_p, (a_2, b_2)_p, \ldots, (a_n, b_n)_p).$$

Set $g_i : P_i \rightarrow R$ a function with the value come from an Abelian ring $R$. Let the vector function $g : P \rightarrow R$ be a function over a meet semi-lattice $P$, $V = (a_1, a_2, \ldots, a_n) \in P$, defined $g(a) = \prod_{i=1}^n g_i(a_i)$. It is apt to the product access to the Abelian ring $R$.

Set $S$, the finite partial order subset of the poset $P$, and $T_i$ the smallest MC finite subset of the poset $P_i$ including in $S_i$. If the direct product $S = S_1 \times S_2 \times \cdots \times S_n$ and $T = T_1 \times T_2 \times \cdots \times T_n$, then the set $T$ is still MC, including in the subset $S$.

Set the Euler’s totient function $\Psi_{S,\phi}$ over set $S$, $T_i$ is a component function of the broad sense Euler’s totient $\Psi_{S,\phi}$-function, then the $\Psi_{S,\phi}$ is the broad sense Euler’s totient $\Psi_{S,\phi}$.
-function defining over Descartes direct product $S$. In addition, $S_i$, $T_i$ are finite subsets, so $S$, $T$ are finite subsets too. Without the generality, let $S = \{d_1, d_2, \ldots, d_n\}$, $T = \{f_1, f_2, \ldots, f_m\}$ then $\Psi_{S,g}(d_i) = g(d_i) = \sum_{j \neq i} m_{ij} \Psi_{S,g}(d_j)$.

Similar to the previous Lemma 1, we have $\Psi_{S,g}(d_i) = \prod_{j=1}^{n} \Psi_{S,g}(d_j)$.

Define the meet matrix $\langle S \rangle_g = (m_{ij})_{q \times q}$ on $S$, where $m_{ij} = g(d_i, d_j)$.

We have restricted the Abelian ring $R$ to the real number field with $g_i : P_i \rightarrow R$, at the same time, let $\Psi_{S,g_i} > 0$. Let $T = T_1 \times T_2 \times \cdots \times T_n$ are the Descartes direct product, the set $T$ is MC and containing the subset $S$, when Euler’s totient function $\Psi_{S,g} > 0$, hence

(i) **(Determinant’s lower bound)** $\det(\langle S \rangle_g) \geq \prod_{d \in S} \Psi_{T,g}(d)$, the equality is fulfilled iff the poset $S$ is MC. Meanwhile, there do not exist the element in the difference set $T \setminus S$ that has fulfilled the partial order relationships $p$ with any one element in the poset $S$.

(ii) **(Determinant’s upper bound)** Set the strong inequality $\det(\langle S \rangle_g) < \prod_{d \in S} g(d)$ is establishment.

That theorem mentioned earlier is necessary about $\Psi_{S,g} > 0$, which is easier to discuss to make $\langle S \rangle_g$ positive definite. But the following theorem is not necessary about $\Psi_{S,g} > 0$, so we can get the following results:

**Theorem 5** Set $S = S_1 \times S_2 \times \cdots \times S_n$ is the Descartes direct product, if the poset $S$ is MC, then the determinant of some meet-matrix $\det(\langle S \rangle_g) = \prod_{d \in S} \Psi_{T,g}(d)$ is establishment.

Comparatively speaking, Theorem 4 and previous Theorem 3 have gotten the same conclusion on the determinant of a meet-matrix, so its proof is omitted. Theorem 5 is also same argument with the Theorem 13 [7]. Similar processing, we won’t talk more about the proof here.

**5 Conclusions**

The gcd-matrices on some sets are a special class of matrices with many beautiful properties. Their determinant calculations are simple and quick, and it helps to design lightweight cryptographic arithmetics and key exchange protocol [27–29]. In addition, the determinant calculation of gcd-matrix is easy to program because of its low computational complexity. Because of its wide application, the gcd-matrix is a valuable long-term research topic. The mixcolumn cryptography characteristics and the maximum branchnumber of gcd-matrices are important research parameters.

The generalized greatest common factor matrices (ggcd-matrix) are a class of special importance and perfection matrices, this article has studied the value of their determinants. We have known that the consummate mathematics relations between generalized greatest common divisor matrices and the generalized Euler’s totient $\Psi_{S,g}$ – function, these relations are taken into account a construction perspective. Our next work goal is to study the eigenvalues, the invariant factor and the characteristic divisor for the generalized greatest common divisor matrix (ggcd-matrix) on the general poset $S$. The relationship between the branch number of meet matrices and the generalized Euler’s totient $\Psi_{S,g}$ – function needs further study. Using meet matrices as the generating matrix to design error correcting codes is an important research field of algebraic coding. That kind of error-correcting code can be constructed the quantum cryptography resisting quantum computation attacks, which is also an important research area of quantum communication.

**Acknowledgements** This research was supported by the following China projects: 1. Educational research project of Hubei Polytechnic University—Research on the overall optimization to the theory and practice course of “the information theory and Coding”(2015B09); 2. Scientific research project of Hubei Polytechnic University—Quantum computing and its application(16xjz02A). Research on automatic design of cryptographic components(11yzj10R); 3. Scientific research project of Hubei Provincial Department of Education—Automatic design of cryptographic components based on orthographic permutations (B2014041), Quantum error-correcting codes and its application in anti-quantum computation cryptography (D20174502); 4. Scientific research project of Science and Technology Department of Hubei Provincial—Design and application of asymmetric algorithms against quantum computation attack in big data environment (2018CFB550).

**Compliance with ethical standards**

**Conflict of interest** We all declare that we have no conflict of interest in this paper.
References

1. Anderson DD, Izumi S, Ohno Y et al (2016) GCD and LCM-like identities for ideals in commutative rings. J Algebra Appl 15(01):12
2. Altunışık E, Büyükköse Şerife (2016) On bounds for the smallest and the largest eigenvalues of GCD and LCM matrices. Math Inequal Appl 19(1):117–125
3. Bourne M, Winkler JR, Su Y (2017) A non-linear structure-preserving matrix method for the computation of the coefficients of an approximate greatest common divisor of two Bernstein polynomials. J Comput Appl Math 320:221–241
4. Bourne M, Winkler JR, Yi S (2017) The computation of the degree of an approximate greatest common divisor of two Bernstein polynomials. Appl Numer Math 111:17–35
5. Rajarama Bhat BV (1991) On greatest common divisor matrices and their applications. Linear Algbera Appl 158:77–97
6. Yun Fan, Hongwei Liu (2002) Group and combination coding. Wuhan University Press, Wuhan
7. Smith HJS (1875–1876) On the value of a certain arithmetical determinant. Proc Lond Math Soc 7:208–212
8. Gashkov SB, Sergeev IS (2016) On the additive complexity of GCD and LCM matrices. Math Notes 100(1–2):199–212
9. Ilmonen Pauliina (2016) On meet hypermatrices and their eigenvalues. Linear Multilinear Algebra 64(5):842–855
10. Korkee I, Haukkanen P (2001) Bounds for determinants of meet matrices associated with incidence functions. Linear Algebra Appl 329:77–88
11. Bourque K, Ligh S (1992) On GCD and LCM matrices. Linear Algebra Appl 174:65–74
12. Bourque K, Ligh S (1993) Matrices associated with arithmetical functions. Linear Multilinear Algebra 34:261–267
13. Bourque K, Ligh S (1993) Matrices associated with classes of arithmetical function. Number Theory 45:367–376
14. Leonetti P, Sanna C (2017) On the greatest common divisor of n and the nth Fibonacci number. Roc Mt J Math. Retrieved from https://arxiv.org/pdf/1704.00151
15. McTague C (2017) On the Greatest Common Divisor of Binomial Coefficients. The American Mathematical Monthly 124(4):353
16. Jacobson N (1974) Basic Algebra I. W.H. Freeman, San Francisco
17. Haukkanen P (1996) On meet matrices on posets. Linear Algebra Appl 249:111–123
18. Rahman MM, Bhuiyan MNAS, Rahim MS et al (2016) A lightweight PAPR reduction scheme using Greatest Common Divisor matrix based SLM technique. In: IEEE 2016 9th international conference on electrical and computer engineering (ICECE), Dhaka, pp 491–494
19. Rahman MM, Rahim MS, Bhuiyan MNAS et al (2015) Greatest common divisor matrix based phase sequence for PAPR reduction in OFDM system with low computational overhead. In: International conference on electrical & electronic engineering (ICEEE), Rajshahi, pp 97–100
20. Stanley RP (1986) Enumerative combinatorics, vol I. Wadsworth and Brooks/cole, Monterey
21. Sarkar M, Ghosal P (2016) Mathematics using DNA: performing GCD and LCM on a DNA computer. In: IEEE international symposium on nanoelectronic and information systems (iNIS), Gwalior, pp 240–243
22. Beslin S, Ligh S (1986) Another generalisation of Smith’s determinant. Bull Austral Math Soc 40:413–415
23. Beslin S, Ligh S (1989) Greatest common divisor matrices. Linear Algebra Appl 118:69–76
24. Beslin S, Ligh S (1992) GCD-closed set and the determinants of GCD matrices. Fibonacci Quart 30:157–160
25. Hong S (1998) Bounds for determinants of Matrices associated with classes of arithmetical functions. Linear Algebra Appl 281:311–322
26. Li Z (1990) The determinants of GCD matrices. Linear Algebra Appl 134:137–143
27. A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. Int J Adv Intell Paradigms 9(2–3):111–121 (2017)
28. A lightweight authenticated encryption scheme based on chaotic scml for railway cloud service. IEEE Access 6:711–722 (2017)
29. ThinORAM: towards practical oblivious data access in fog computing environment. IEEE Trans Serv Comput (2019)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.