1. Computability, Complexity and Algorithms

Consider two sets A and B, each having n integers in the range from 0 to $8n$ where n is a power of 2. We wish to compute the *Cartesian sum* of A and B, defined by:

$$C = \{x + y : x \in A \text{ and } y \in B\}.$$

We want to find the set of elements in C and also the number of times each element of C is realized as a sum of elements in A and B.

Part (a): Give an algorithm to compute the Cartesian sum C **by a reduction to FFT**. State the running time (as fast as possible in $O()$ notation).

Part (b): Extend your algorithm to obtain the number of times each $i \in C$ is realized as a sum of elements in A and B.

Example: for $A = [1, 2, 3]$ and $B = [2, 3]$ then $C = [3, 4, 5, 6]$ and the solution to the Cartesian Sum problem is:

3 appears and is obtainable in 1 way,
4 appears and is obtainable in 2 ways,
5 appears and is obtainable in 2 ways,
6 appears and is obtainable in 1 way.

Solution: Let

$$A(x) = \sum_{i \in A} x^i \text{ and } B(x) = \sum_{i \in B} x^i.$$

Note, these polynomials are of degree $\leq 8n$. Hence, denote their respective coefficients as the vectors $a = (a_0, \ldots, a_{8n})$ and $b = (b_0, \ldots, b_{8n})$. Next we compute the product polynomial $C(x) = A(x) \times B(x)$ using FFT. Specifically, we run FFT on the vectors a and b with the $16n$-th roots of unity. We multiply these values to get $C(x)$ at the $16n$-th roots of unity. Then we run inverse FFT to get the coefficients of $C(x)$. Denote these coefficients as $c = (c_0, \ldots, c_{16n})$. For all $0 \leq i \leq 16n$, if $c_i > 0$ then $i \in C$ and it can be obtained in c_i ways. The running time is $O(n \log n)$.

2. Analysis of Algorithms

Recall that computing the number of perfect matchings in a graph $G = (V, E)$ is #P-complete. For this problem assume that you are given an oracle that returns the number of perfect matchings in a given graph in one time step.

(i) A graph is said to be *matching covered* if every edge of it participates in some perfect matching. Given graph $G = (V, E)$ show how to obtain, in polynomial time, a subgraph $G' = (V, E')$, with $E' \subseteq E$ such that G' is matching covered and the number of perfect matchings in G and G' is the same.

Recall that the perfect matching polytope for a bipartite graph $G = (V, E)$ is defined in $\mathbb{R}^E$ and is given by the following set of linear equalities and inequalities.

$$\begin{aligned} x(\delta(v)) &= 1 \quad \forall v \in V, \\ x_e &\geq 0 \quad \forall e \in E. \end{aligned} \tag{1}$$

The equation says that the total x value of edges incident at each vertex v is 1.

(ii) Give a polynomial time algorithm for finding a point in the interior of the perfect matching polytope for a connected, matching covered bipartite graph $G = (V, E)$.

Solution: (i) Let $\mathcal{O}$ denote the oracle and $\#G$ the number of perfect matchings in G. First call $\mathcal{O}(G)$ to find $\#G$. For each edge $e \in E$: remove e and find the number of perfect matchings in the remaining graph. If the number is the same as $\#G$, remove e forever, else leave e in G. The resulting graph, say G', is matching covered and has the same number of perfect matchings as G.

(ii) For edge $e \in E$, let $\#G_e$ denote the number of perfect matchings that e participates in. Also let $G'_e = (V, E - e)$. First call $\mathcal{O}(G)$ to find $\#G$. Next, for each edge $e \in E$, call $\mathcal{O}(G'_e)$; this will return $\#G - \#G_e$. Hence $\#G_e$ can be computed for each $e \in E$.

Finally, output the point x such that

$$x_e = \frac{\#G_e}{\#G}.$$

This point satisfies all constraints of the perfect matching polytope for $G = (V, E)$. Since G is connected and matching covered, the degree of each vertex is at least 2. Therefore, for each edge e, $0 < x_e < 1$. Hence this point lies in its interior of the polytope.

3. Theory of Linear Inequalities

Let $P = \{x \in \mathbb{R}^n \mid Ax \leq b\} \subseteq [0,1]^n$ with $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$ be a polytope contained in the 0/1 cube; in particular the bound inequalities $0 \leq x \leq 1$ are valid for P.

For $i \in [n]$ we consider the following procedure:

1. Generate the nonlinear system $(b - Ax)x_i \geq 0$, $(b - Ax)(1 - x_i) \geq 0$.
2. Relinearize the system by replacing $x_j x_i$ with y_j whenever $i \neq j$ and x_j whenever $i = j$. We obtain a new, higher dimensional polyhedron M_i.
3. Define $P_i := \text{proj}_x M_i$.

Finally define $P^1 := \bigcap_{i \in [n]} P_i$. This polyhedron is a strengthening of the original formulation of P.

Prove the following:

$$\text{conv}(P \cap \{0,1\}^n) \subseteq P^1 \subseteq P.$$

Solution: It suffices to verify the claims separately for each P_i with $i \in [n]$. First observe that $P_i \subseteq P$: every row $A_j x \leq b_j$ of the system $Ax \leq b$ can be obtained by adding up $(b_j - A_j x)x_i \geq 0$ and $(b_j - A_j x)(1 - x_i) \geq 0$. So $A_j x \leq b_j$ is valid for M_i. Moreover, as $A_j x \leq b_j$ only involves x-variables it is also valid for the projection of M_i.

Now we will show that $P_I \subseteq P_i$. As P_i is a polyhedron as a projection of the polyhedron M_i, it suffices to consider a 0/1 vertex $\bar{x}$ of P_I. For this we define a new point $(\bar{x}, y) \in M_i$ that projects to $\bar{x}$. For this we define $y_j = \bar{x}_j \bar{x}_i$ for all $i \neq j$ and we claim that $(\bar{x}, y) \in M_i$. With this we can reverse the substitution in Step 2 (as $\bar{x} \in \{0,1\}^n$ and so $x_i^2 = x_i$) and we see that the nonlinear system in Step 1 is trivially satisfied. Step 2 is a relaxation of the feasible region of the nonlinear system in Step 1 and so we have indeed $(\bar{x}, y) \in M_i$ which concludes the proof.

4. Combinatorial Optimization

Given an integer n, let $\mathcal{M}_k = (U, \mathcal{I}_k)$ be a matroid for each $1 \leq k \leq n$ with $\mathcal{M}_k^* = (U, \mathcal{I}_k^*)$ its dual matroid. Consider the matroid $\mathcal{N} = (U, \mathcal{I})$ defined as $\mathcal{N} := (\mathcal{M}_1^* \vee \ldots \vee \mathcal{M}_n^*)^*$,i.e., it is the dual of the union of matroids $\mathcal{M}_1^*, \ldots \mathcal{M}_n^*$.

1. (4 points) Show that
$$\mathcal{I} \subseteq \bigcap_{k \in \{1,\ldots,n\}} \mathcal{I}_k.$$

2. (4 points) Let $(P_1, \ldots, P_n)$ denote a partition of U, i.e. $\cup_{k=1}^n P_k = U$ and each element of U appears in exactly one P_k. Let $b_1, \ldots, b_n$ be positive integers such that $|P_k| \geq b_k$ for each $1 \leq k \leq n$. For every $1 \leq k \leq n$, consider the matroid $\mathcal{M}_k = (U, \mathcal{I}_k)$ where some subset S of U is in $\mathcal{I}_k$ if $|S \cap P_k| \leq b_k$ (observe that there is no restriction on elements not in P_k). Show that the matroid $\mathcal{N}$ as defined above is a partition matroid in the this case. Moreover, show that equality holds in the above containment.

3. (2 points) Give an example where equality does not hold in the containment in (a).

Solution:

1. Since both set families are downward closed, it is enough to argue the containment for the maximal sets in $\mathcal{I}$. Let $A \in \mathcal{I}$ be a basis of $\mathcal{N}$. This implies $U \setminus A$ is a basis of the matroid $\mathcal{N}' := \mathcal{M}_1^* \vee \ldots \vee \mathcal{M}_n^*$. Thus there exists independent sets B_k of $\mathcal{M}_k^*$ for each $1 \leq k \leq n$ such that $U \setminus A = \cup_{k=1}^n B_k$. Since $U \setminus A$ is basis of $\mathcal{N}'$, we can assume that B_k is a basis of $\mathcal{M}_k^*$ without loss of generality. Thus $A = \cap_{k=1}^n (U \setminus B_k)$ and therefore $A \subseteq U \setminus B_k$. But $U \setminus B_k$ is a basis of $\mathcal{M}_k$. Thus $A \in \mathcal{I}_k$ for each k.

2. We apply the definition of dual matroid and matroid union. The basis of $\mathcal{M}_k$ are sets S such that $S \supseteq U \setminus P_k$ and $|S \cap P_k| = b_k$. For any k, the dual matroid $\mathcal{M}_k^* = (U, \mathcal{I}_k^*)$ contains a set $S \in \mathcal{I}_k^*$ if $S \subseteq P_k$ and $|S \cap P_k| \leq |S| - b_k$. Let $\mathcal{N}' = \mathcal{M}_1^* \vee \ldots \vee \mathcal{M}_n^*$. Then a set S is independent in $\mathcal{N}'$ if $|S \cap P_k| \leq |S| - b_k$ for each $1 \leq k \leq n$. Now, the dual matroid $\mathcal{N}$ contains exactly those sets as independent if $|S \cap P_k| \leq b_k$ for each $1 \leq k \leq n$. Thus $\mathcal{N}$ is a partition matroid. Equality holds since $S \in \bigcap_{k \in \{1,\ldots,n\}} \mathcal{I}_k$ iff $|S \cap P_k| \leq b_k$.

3. We will consider the simplest case of $n = 2$ where the two matroids are defined as above but P_1 and P_2 intersect non-trivially. Let $U = \{x, y, z\}$. Let $P_1 = \{x, y\}$ and $P_2 = \{y, z\}$. Let $b_1 = b_2 = 1$. Let $\mathcal{M}_k = (U, \mathcal{I}_k)$ contain sets such that $|S \cap P_k| \leq 1$. Thus

$$\mathcal{I}_1 = \{\{\}, \{x\}, \{y\}, \{z\}, \{x, z\}, \{y, z\}\},$$

$$\mathcal{I}_2 = \{\{\}, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}\}.$$

Therefore,

$$\mathcal{I}_1 \cap \mathcal{I}_2 = \{\{\}, \{x\}, \{y\}, \{z\}, \{x, z\}\}.$$

It is easy to see $\mathcal{I}_1 \cap \mathcal{I}_2$ is not a collection of independent sets of a matroid. This follows since the exchange property is violated for $\{y\}$ and $\{x, z\}$. Thus the equality cannot hold.

5. Graph Theory

Consider the graphs G in which every induced subgraph H has the property that the vertex-set of every maximal complete subgraph of H intersects every maximal independent set in H.

1. Prove that every such graph G is perfect.
2. Prove that these graphs G are precisely the graphs with no induced subgraph isomorphic to the path on four vertices.

Solution: To prove that G is perfect let H be an induced subgraph of G. We show that $\chi(H) = \omega(H)$ by induction on $\omega(H)$. The assertion clearly holds when $\omega(H) = 1$, and so we may assume that $\omega(H) > 1$ and that the assertion holds for all induced subgraphs H' of H with $\omega(H') < \omega(H)$. Let I be a maximal independent set in H. By hypothesis $\omega(H \backslash I) < \omega(H)$. Thus $\chi(H \backslash I) = \omega(H \backslash I) < \omega(H) \leq \chi(H)$ by the induction hypothesis. By adding I as a color class to a $\chi(H \backslash I)$-coloring of $H \backslash I$ we find that $\chi(H) \leq \omega(H)$, as desired.

To prove the second assertion let x, y, z, w be the vertices of a 4-vertex path P in order. Then $\{y, z\}$ is the vertex-set of a maximal complete subgraph of P and $\{x, w\}$ is a maximal independent set disjoint from $\{y, z\}$.

To prove the converse let I be a maximal independent set in an induced subgraph H of G and let Q be the vertex-set of a maximal complete subgraph of H such that $I \cap Q = \emptyset$, and suppose for a contradiction that H has no induced subgraph isomorphic to the path on four vertices. For $v \in Q$ let $N(v)$ denote the set of neighbors of v in I. Then for distinct $u, v \in Q$ we have that either $N(u) \subseteq N(v)$ or $N(v) \subseteq N(u)$, for if $v' \in N(v) - N(u)$ and $u' \in N(u) - N(v)$, then $\{v', v, u, u'\}$ is the vertex-set of an induced path in H, a contradiction. Let $v \in Q$ be such that $N(v)$ is minimal. We have $N(v) \neq \emptyset$, for otherwise $I \cup \{v\}$ contradicts the maximality of I. Let $x \in N(v)$. The minimality of $N(v)$ implies that $x \in N(u)$ for every $u \in Q$. But now $Q \cup \{x\}$ contradicts the maximality of Q.

6. Probabilistic methods

Let $B_{n,n,p}$ denote the random *bipartite* graph with n vertices in each part, where an edge connecting two vertices in different parts is included independently with probability p (and there are no edges connecting vertices in the same part). Let X be the random variable which counts the number of 4-cycles in $B_{n,n,p}$. Use Janson's inequality (or extended Janson's inequality) to prove bounds of the form

$$\Pr[X = 0] \le \mathrm{e}^{-\Omega(n^x p^y)}$$

(a) if $0 < p < 1$ is a constant.

(b) if $0 < p = p(n) < 1$ is a function of n
(Hint: you might want to distinguish different ranges of p, e.g., where $n^{-\alpha} \ll p \ll n^{-\beta}$ holds for suitable $\alpha, \beta > 0$)

Solution: Let V_1 and V_2 denote the two parts of size n in $B_{n,n,p}$. Observe that $B_{n,n,p}$ has n^2 many edges in total. As usual, we view $B_{n,n,p}$ as the product of n^2 smaller probability spaces, one for each possible edge. For every possible 4-cycle $S \subseteq K_{n,n}$, let X_S be the indicator variable which takes the value 1 iff all four edges are present in $B_{n,n,p}$. Thus the coordinates I_S from Janson's inequality are exactly the four edges of the cycle S. Clearly, X_S only depends on these. Moreover, clearly we have

$$\Pr[X_S] = p^4 \ .$$

Let now

$$X = \sum_{S \text{ possible 4-cycle}} X_S$$

denote the number of 4-cycles in $B_{n,n,p}$. Since we need to pick exactly two vertices from both V_1 and V_2 to obtain a 4-cycle, the sum has $\Theta(n^2) \cdot \Theta(n^2) = \Theta(n^4)$ many terms. By linearity of expectation we obtain

$$\mu = \mathbb{E}[X] = \Theta(n^4 p^4) \ .$$

In order to apply Janson's inequality we have to calculate Δ and in particular the terms $\Pr[X_S = 1 \wedge X_T = 1]$. Observe that I_S and I_T intersect in either 1 or 2 vertices since in all other cases S and T are either disjoint or equal.

For $|I_S \cap I_T| = 1$, S and T share exactly one edge. Once the intersecting edge is fixed there are $\Theta(n^2) \cdot \Theta(n^2) = \Theta(n^4)$ many ways to extend it to S and T such that they do not share any further edges (we simply have to pick two extra vertices in both V_1 and V_2). As there are n^2 edges we obtain that in total there are $\Theta(n^2) \cdot \Theta(n^4) = \Theta(n^6)$ pairs S, T with $|I_S \cap I_T| = 1$. By counting the edges we obtain that $\Pr[X_S = 1 \wedge X_T = 1] = p^7$ for these pairs.

For $|I_S \cap I_T| = 2$, S and T share exactly two edges. It is easily seen that this is only possible if the two common edges are incident. We assume that the two edges meet in a vertex of V_1 – clearly, the other case is symmetric. Observe that there are $\Theta(n) \cdot \Theta(n^2) = \Theta(n^3)$ many ways to fix such a pair of edges. Once the intersecting edges are fixed there are $\Theta(n^2)$ many ways to extend them to S and T such that they do not share any further edges. Hence there are $\Theta(n^5)$

many pairs S, T with $|I_S \cap I_T| = 2$. By counting the edges we obtain $\Pr[X_S = 1 \wedge X_T = 1] = p^6$ for these pairs.

Putting it all together, we obtain that

$$\Delta = \Theta(n^6p^7) + \Theta(n^5p^6) = \begin{cases} \Theta(n^6p^7) & p \gg n^{-1} \\ \Theta(n^5p^6) & p \ll n^{-1}. \end{cases}$$

If $0 < p < 1$ is a constant we have $\mu = \Theta(n^4)$ and $\Delta = \Theta(n^6)$, and thus $\Delta \geq \mu$ for n large enough. Using Janson's inequality we obtain

$$\Pr[X = 0] \leq \mathrm{e}^{-\mu^2/2\Delta} = \mathrm{e}^{-\Omega(n^2)} \quad ,$$

which solves (a).

If $0 < p = p(n) < 1$ is a function of n, then we first note that $\mu \gg \Delta$ when $p \ll n^{-2/3}$ and $\mu \ll \Delta$ when $p \gg n^{-2/3}$. Combining Janson's inequality with extended Janson's inequality (which give good bounds for, say, $\mu \geq \Delta$ and $\mu \leq \Delta$, respectively), it follows that, say,

$$\Pr[X = 0] \leq \begin{cases} \mathrm{e}^{-\Omega(\mu)} & p \ll n^{-2/3}, \\ \mathrm{e}^{-\Omega(\mu^2/\Delta)} & p \gg n^{-2/3}. \end{cases}$$

Noting that

$$\frac{\mu^2}{\Delta} \overset{(p \gg n^{-2/3})}{=} \frac{\Theta(n^8p^8)}{\Theta(n^6p^7)} = \Theta(n^2p),$$

as well as

$$\mu = \Theta(n^4p^4) \overset{(p \ll n^{-1})}{\ll} 1,$$

in view of the trivial bound $\Pr[X = 0] \leq 1$ we altogether we obtain that

$$\Pr[X = 0] \leq \min\{e^{-\frac{\Theta(n^8p^8)}{\mu + \Delta}}, 1\} = \begin{cases} \mathrm{e}^{-\Omega(n^2p)} & p \gg n^{-2/3} \\ \mathrm{e}^{-\Omega(n^4p^4)} & n^{-1} \ll p \ll n^{-2/3} \\ 1 & p \ll n^{-1}, \end{cases}$$

which solves (b).

7. Algebra

Let p be a prime and $\mathbb{F}_q$ be a field with p^d elements. Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be the map $f(x) = x^p$ for all x in $\mathbb{F}_q$. Show that there exists an element x in $\mathbb{F}_q$ such that $\{x, fx, \ldots, f^{d-1}x\}$ is a basis for $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space.

Solution: $\mathbb{F}_q$ is a module over $\mathbb{F}_p[T]$ with T acting by f. We claim that the minimal polynomial of f is $T^d - 1$. Since $\mathbb{F}_q^\times$ is an abelian group of order $p^d - 1$, we have that $x^{p^d - 1} = 1$, thus $x^{p^d} = x$, showing that $f^d = 1$. Thus the minimal polynomial of f must divide $T^d - 1$. Let $g(T)$ be a factor of $T^d - 1$ of degree less than d. Then $g(f)(x)$ is a polynomial of degree less than p^d. Since $\mathbb{F}_q$ is a field, $g(f)(x)$ has fewer than p^d roots in $\mathbb{F}_q$. Thus $g(T)$ is not the minimal polynomial of f, and it follows that $T^d - 1$ is the minimal polynomial of f as claimed. Since the minimal polynomial has degree d, it must also be the characteristic polynomial. By the classification of modules over PIDs, it follows that $\mathbb{F}_q \cong \mathbb{F}_p[T]/\langle T^d - 1\rangle$ as $\mathbb{F}_p[T]$-modules. The basis $\{1, T, \ldots, T^{d-1}\}$ of the right hand side as an $\mathbb{F}_p$-vector space corresponds to a basis $\{x, fx, \ldots, f^{d-1}x\}$ of the left hand side.

7. Linear Algebra

Notation. For a matrix $A \in \mathbb{R}^{n\times n}$, we write $A \geq 0$ to mean that all the entries of A are nonnegative numbers.

Consider a matrix $A \in \mathbb{R}^{n\times n}$ satisfying these conditions (this is called an *M-matrix*):

(i) for all $i, j = 1, \ldots, n$, and $i \neq j$, $a_{ij} \leq 0$;

(ii) we can write $A = sI - B$, where $B \geq 0$, and $s \geq \rho(B)$.

Further, A is an invertible M-matrix if, in part (ii), $s > \rho(B)$. Prove that
A is an invertible M-matrix if and only if $A^{-1} \geq 0$.

Solution: Assume that A is an invertible M-matrix. Then $A = sI - B$, with $s > \rho(B)$ and $B \geq 0$. So, $A = s(I - B/s)$ and $\rho(I - B/s) < 1$, so that $(I - B/s)$ is convergent. Therefore, A^{-1} exists and

$$A^{-1} = \frac{1}{s}\sum_{k=0}^{\infty}(B/s)^k \ ,$$

and since all terms on the right hand side are matrices with nonnegative entries, then $A^{-1} \geq 0$.

Conversely, assume that $A^{-1} \geq 0$. Let $C = A^{-1}$. From the relation $CA = I$, looking at the (i, i) element, and using that $a_{ij} \leq 0$ for $i \neq j$, one has

$$\sum_{j=1}^{n} c_{ij}a_{ji} = c_{ii}a_{ii} - \sum_{j\neq i} c_{ij}|a_{ji}| = 1$$

from which $a_{ii} > 0$ for all $i = 1, \ldots, n$.
Now, write $A = D + A_{\text{off}}$, where D is the diagonal matrix with the diagonal entries of A and A_{off} is the matrix A with 0's replacing its diagonal entries, and let $s = \max_i a_{ii}$. Therefore:

$$A = sI + [(D - sI) + A_{\text{off}}] = sI - [(sI - D) - A_{\text{off}}] = sI - B \ ,$$

with $B \geq 0$. Now we prove that $s > \rho(B)$, knowing that $A^{-1} = (sI - B)^{-1} \geq 0$.

Since $B \geq 0$, using Frobenius theorem, let $x \geq 0$, $x \neq 0$, be an eigenvector of B such that $Bx = \rho(B)x$, and therefore $(sI - B)x = (s - \rho(B))x$. Since $(sI - B)$ is invertible, one has

$$(s - \rho(B))\,(sI - B)^{-1}x = x \ ,$$

and since $(sI - B)^{-1} \geq 0$ and $x \geq 0$, but $x \neq 0$, then $s - \rho(B) > 0$.