数学-HYX

三种集合幂卷积的正变换和逆变换

```
void fwtXor(ll* a, int len) {
    if(len == 1) return;
    int h = len \gg 1;
    fwtXor(a, h);
    fwtXor(a + h, h);
    for(int i = 0; i < h; ++i) {
        11 x1 = a[i];
        11 	ext{ } x2 = a[i + h];

a[i] = (x1 + x2) 	ext{ } MOD;
        a[i + h] = (x1 - x2 + MOD) \% MOD;
void ifwtXor(11* a, int len) {
    if(len == 1) return;
    int h = len >> 1;
    for(int i = 0; i < h; ++i) {
        // y1=x1+x2
// y2=x1-x2
        11 \ y1 = a[i];
        11 y2 = a[i + h];
        a[i] = (y1 + y2) * invTwo % MOD;
        a[i + h] = (y1 - y2 + MOD) * invTwo % MOD;
    ifwtXor(a, h);
    ifwtXor(a + h, h);
void fwtAnd(ll* a, int len) {
    if(len == 1) return;
    int h = len \gg 1;
    fwtAnd(a, h);
    fwtAnd(a + h, h);
    for (int i = 0; i < h; ++i) {
        ll x1 = a[i];
        11 x2 = a[i + h];
        a[i] = (x1 + x2) \% MOD;
        a[i + h] = x2;
void ifwtAnd(ll* a, int len) {
    if(len == 1) return;
    int h = 1en \gg 1;
    for(int i = 0; i < h; ++i) {
        // y1=x1+x2
// y2=x2
        11 y1 = a[i];
        11 \ y2 = a[i + h];
        a[i] = (y1 - y2 + MOD) \% MOD;
        a[i + h] = y2;
    ifwtAnd(a, h);
    ifwtAnd(a + h, h);
void fwtOr(ll* a, int len) {
    if(len == 1) return;
    int h = len \gg 1;
    fwt0r(a, h);
    fwt0r(a + h, h);
    for(int i = 0; i < h; ++i) {
    11 x1 = a[i];
        11 x2 = a[i + h];
        a[i] = x1;
        a[i + h] = (x2 + x1) \% MOD;
void ifwtOr(11* a, int len) {
    if(len == 1) return;
    int h = len \gg 1;
    for(int i = 0; i < h; ++i) {
        // y1=x1
// y2=x2+x1
        11 y1 = a[i];
        11 y2 = a[i + h];
        a[i] = y1;
        a[i + h] = (y2 - y1 + MOD) \% MOD;
    ifwt0r(a, h);
    ifwt0r(a + h, h);
```

大步小步算法

```
struct Node {
   11 x, y;
vector <Node> G[MAX];
11 hash(11 a) {
   return a % MOD;
11 find(11 a) {
   11 u = hash(a);
    for (ll i = 0; i < G[u].size(); i++) {
        if (G[u][i].x == a) return G[u][i].y;
   return -1LL;
void init() {
   for (11 i = 0; i \le MOD; i++) G[i].clear();
11 mod_mul(11 a, 11 b, 11 N) {
    11 \text{ ret = 0};
    while(b) {
       if(b & 1) ret = (ret + a) % N;
       a = 2 * a \% N;
       b >>= 1;
    return ret;
11 mod pow(11 x, 11 n, 11 N) {
   11 ret = 1;
    x \% = N;
    while(n)
       if (n & 1) ret = mod mul(ret, x, N);
       x = mod_mul(x, x, N);
       n >>= 1;
   }
   return ret;
void ex_gcd(11 a, 11 b, 11& d,11& x, 11& y) {
   if (b == 0) {
       d = a;
       x = 1;
       y = 0;
       return;
    ex_gcd(b, a\%b, d, y, x);
   y = x * (a / b);
11 inv(11 a, 11 N){
   11 d, x, y;
    ex_gcd(a, N, d, x, y);
    if (d == 1) return (x + N) \% N;
    return -1;
// 大步小步算法求 a ^ x = b mod N 中的 x
11 mod_log(11 a, 11 b, 11 N){
    11 \text{ m} = (11) \operatorname{sqrt} (N + 0.5);
    11 s = 1LL;
    for (11 i = 0; i \le m; i++) {
        if(find(s) < 0) {
            G[hash(s)].push_back((Node) \{s, i\});
        s = mod_mul(s, a, N);
    11 v = inv(mod_pow(a, m, N), N);
                                                          //求a^m的逆元
    for (11 i = 0; i < m; i++) {
        11 res = find(b);
        if (res != -1) return i * m + res;
       b = mod_mul(b, v, N);
    return -1LL; //无解
轮廓线dp,n*m填1*2
int n, m, cur;
ull dp[2][(1 << 10) + 5];
void update(int past, int now) {
    if (now \gg m & 1) dp[cur][now \hat{} (1 << m)] = (dp[cur][now \hat{} (1 << m)] + dp[1-cur][past]);
int main() {
    while(scanf("%d%d", &n, &m) != EOF) {
        if (n < m) swap (n, m);
```

```
cur = 0;
         dp[0][(1 << m) - 1] = 1;
         for (int i = 0; i < n; i++) {
             for(int j = 0; j < m; j++) {
                  cur ^= 1;
                  CLR(dp[cur]);
                  for(int state = 0; state \langle 1 \langle \langle m; state^{++} \rangle \rangle
                      update(state, state << 1); if(i && !((1 << m - 1) & state)) update(state, (state << 1) ^ (1 << m) ^ 1);
                      if(j && !(state & 1)) update(state, (state << 1) \hat{\ } 3);
         }
         printf("%1lu\n", dp[cur][(1 << m) - 1]);
    return 0;
CDQ-NTT
const int N = 5e5 + 10, INF = 0x3f3f3f3f, MOD = 1004535809;
const int G = 3, P = 1004535809; // MOD的原根, 当且仅当 g^(MOD-1) = 1 % MOD
typedef long long 11;
11 Pow(11 x, 11 n) {
    11 \text{ ret} = 1;
    for(; n; n >>= 1) {
         if(n & 1) ret = ret * x \% P;
         x = x * x \% P;
    return ret;
11 A[N], B[N];
void rader(11* y, int len) {
    for (int i = 1, j = len / 2; i < len - 1; i++) {
         if(i < j) swap(y[i], y[j]);</pre>
         int k = len / 2;
while(j >= k) {j -= k; k /= 2;}
         if(j < k) j += k;
void ntt(11* y, int len, int op) {
    rader(y, len);
    for(int h = 2; h \le len; h \le 1) {
         11 wn = Pow(G, (P - 1) / h);
         if (op == -1) wn = Pow(wn, P - 2);
         for (int j = 0; j < len; j += h) {
             11 \text{ w} = 1;
             for (int k = j; k < j + h / 2; k++) {
                  11 u = y[k];
                  11 t = w * y[k + h / 2] \% P;
                  y[k] = (u + t) \% P;

y[k + h / 2] = (u - t + P) \% P;
                  w = w * wn \% P;
        }
    if(op == -1) {
         11 \text{ inv} = \text{Pow}(\text{len, P} - 2);
         for(int i = 0; i < len; i++) y[i] = y[i] * inv % P;
11 f[N], g[N];
// dp[i] = (i-1)! * sigma(a[j] * b[i-1-j])
void cdq(int 1, int r) {
    if(\hat{l} = r) return;
    int mid = (1 + r) >> 1;
    cdq(1, mid);
    int len = 1;
    while (len \leq r - 1 + 1) len \leq 1;
    for (int i = 0; i < len; i++) {
         A[i] = a[i];
         B[i] = (1 + i \le mid ? finv[1 + i] * f[1 + i] % P : 0);
    ntt(A, len, 1);
    ntt(B, len, 1);
for(int i = 0; i < len; i++) A[i] = A[i] * B[i] % P;
    ntt(A, len, -1);
```

```
for(int_i = mid + 1; i <= r; i++) {
       f[i] += fact[i - 1] * A[i - 1 - 1] % P;
       f[i] %= P;
   cdq(mid + 1, r);
快速计算1-n素数个数
#define MAXN 100
#define MAXM 50010
#define MAXP 666666
#define MAX 1000001
#define clr(ar) memset(ar, 0, sizeof(ar))
#define isprime(x) (( (x) && ((x)&1) && (!chkbit(ar, (x)))) || ((x) == 2))
namespace pcf {
long long dp[MAXN][MAXM];
unsigned int ar[(MAX >> 6) + 5] = \{0\};
int len = 0, primes[MAXP], counter[MAX];
void Sieve() {
    setbit(ar, 0), setbit(ar, 1);
        for(int i = 3; (i * i) < MAX; i++, i++) {
           if(!chkbit(ar, i)) {
               int k = i \ll 1;
               for(int j = (i * i); j < MAX; j += k) setbit(ar, j);
           }
        }
        for (int i = 1; i < MAX; i++) {
           counter[i] = counter[i - 1];
if(isprime(i)) primes[len++] = i, counter[i]++;
   void init() {
        Sieve();
        for (int n = 0; n < MAXN; n++) {
           for (int m = 0; m < MAXM; m^{++}) {
               if(!n) dp[n][m] = m;
               else dp[n][m] = dp[n-1][m] - dp[n-1][m / primes[n-1]];
       }
   }
    long long phi(long long m, int n) {
        if (n == 0) return m;
        if (primes[n-1] >= m) return 1;
        if(m < MAXM && n < MAXN) return dp[n][m];</pre>
        return phi(m, n-1) - phi(m / primes[n-1], n-1);
   long long Lehmer(long long m)
        if(m < MAX) return counter[m];</pre>
        long long w, res = 0;
        int i, a, s, c, x, y;
        s = sqrt(0.9 + m), y = c = cbrt(0.9 + m);
       a = counter[y], res = phi(m, a) + a - 1;
       for(i = a; primes[i] <= s;
               i++) res = res - Lehmer(m / primes[i]) + Lehmer(primes[i]) - 1;
        return res;
long long solve(long long n) {
    int i, j, k, 1;
    long long x, y, res = 0;
    for (i = 0; i < pcf::len; i++) {
       x = pcf::primes[i], y = n / x;
        if((x * x) > n) break;
        res += (pcf::Lehmer(y) - pcf::Lehmer(x));
    for(i = 0; i < pcf::len; i++) {
       x = pcf::primes[i];
        if((x * x * x) > n) break;
       res++:
```

```
return res;
// 初始化
pcf::init();
// 调用输出1-n的素数个数
cout << pcf::Lehmer(n) << endl;</pre>
中国剩余定理
void exgcd(l1 a, l1 b, l1& d, l1& x, l1& y) {
   if(!b) {d = a; x = 1; y = 0;}
    else \{ exgcd(b, a\%b, d, y, x); y = x * (a / b); \}
ll inv(ll a, ll n) { //mod n
    11 d, x, y;
    exgcd(a, n, d, x, y);
return d == 1 ? (x + n) % n : -1;
/*
x = ai \pmod{mi}
m1 * m2 * \dots * mi = M
mi之间互素
x = sigma(ai * Mi * Mi(-1)) % M
Mi = M / mi
Mi(-1) = Mi 模mi的逆
11 mul(11 a, 11 b, 11 M) {
    11 ret = 0;
    while(b) {
        if(b & 1) ret = (ret + a) % M;
        a = a * 2 \% M;
        b \gg 1;
    return ret;
11 CRT(11 a[], 11 m[], 11 n) {
    11 M = 1;
    11 \text{ ans} = 0;
    for(int i = 1; i \le n; i \leftrightarrow n
        M = m[i];
    for (int i = 1; i \le n; i++) {
        11 Mi = M / m[i];
        11 x, y, d;
        exgcd(Mi, m[i], d, x, y);
        ans = (ans + mul(x, mul(a[i], Mi, M), M)) % M;
    if (ans < 0) ans += M;
    return ans;
/*
当mi不互素的时候
两两合并求答案
*/
bool Merge(11 a1, 11 m1, 11 a2, 11 m2, 11 &a3, 11 &m3)
    11 d = __gcd(m1, m2);
11 c = a2 - a1;
    if(c % d) return false;
    c = (c \% m2 + m2) \% m2;
    m1 /= d;
    m2 /= d;
    c /= d;
    c *= inv(m1, m2);
    c %= m2;
    c *= m1 * d;
    c += a1;
    m3 = m1 * m2 * d;
    a3 = (c \% m3 + m3) \% m3;
    return true;
11 CRT(11 a[], 11 m[], int n) {
    11 \ a1 = a[1];
    11 \ m1 = m[1];
    for(int i=2; i \le n; i++) {
        11 \ a2 = a[i];
        11 m2 = m[i];
        11 m3, a3;
        if(!Merge(a1, m1, a2, m2, a3, m3))
            return -1;
        a1 = a3;
        m1 = m3;
    return (a1 % m1 + m1) % m1;
```

```
}
FFT
struct Virt {
    double r, i;
    \label{eq:Virt} Virt\left(double \_r = 0, \ double \_i = 0\right) : r(\_r), \ i\left(\_i\right) \ \{\}
    Virt operator+ (Virt& rhs) {
        return Virt (r + rhs. r, i + rhs. i);
    Virt operator- (Virt& rhs) {
        return Virt(r - rhs.r, i - rhs.i);
    Virt operator* (Virt& rhs) {
        return Virt(r * rhs.r - i * rhs.i, r * rhs.i + i * rhs.r);
};
void Rader(Virt F[], int len) {
    int j = len \gg 1;
    for (int i = 1; i < len - 1; i++) {
         if(i < j) swap(F[i], F[j]);
         int k = len \gg 1;
         while(j \ge k) {
             j -= k;
             k \gg 1;
         if(j < k) j += k;
void FFT(Virt F[], int len, int on) {
    Rader(F, len);
    for(int h = 2; h \le 1en; h \le 1) {
         Virt wn(cos(-on*2*PI/h), sin(-on*2*PI/h));
         for(int j = 0; j < len; j += h) {
             Virt w(1, 0);
             for (int k = j; k < j + h / 2; k++) {
                  Virt u = F[k];
                  Virt t = w * F[k + h / 2];
                  F[k] = u + t;
                  F[k + h / 2] = u - t;
                  w = w * wn;
        }
    if(on == -1)
         for(int_i = 0; i < len; i++)
             F[i].r /= len;
// 黑科技, FFT取膜 cov(p, q)
void Cov(int p[], int q[], int m) {
    int t = sqrt(MOD), len = 1;
    while (len \langle 2 * m \rangle len \langle \langle = 1 \rangle;
    for(int i = 0; i < len; i++) {
         \begin{array}{l} p1[i] = (i < m ? p[i] / t : 0); \\ p2[i] = (i < m ? p[i] % t : 0); \end{array}
        p3[i] = 0;
        \label{eq:fft} \text{FFT}(\text{p1, len, 1}), \ \text{FFT}(\text{p2, len, 1}), \ \text{FFT}(\text{q1, len, 1}), \ \text{FFT}(\text{q2, len, 1});
    for (int i = 0; i < len; i++)
         p3[i] = p1[i] * q2[i] + p2[i] * q1[i];
         p1[i] = p1[i] * q1[i];
         p2[i] = p2[i] * q2[i];
    FFT(p1, len, -1), FFT(p2, len, -1), FFT(p3, len, -1);
    for (int i = 0; i < len; i++) {
         11 t1 = p1[i].r + 0.5;
         11 t2 = p2[i].r + 0.5;
         11 t3 = p3[i].r + 0.5;
         p[i] = (t1 * t * t + t * t3 + t2) \% MOD;
    for(int i = m; i < len; i++) {
        p[i\%m] = (p[i\%m] + p[i]) \% MOD;
        p[i] = 0;
康拓展开
int fac[10] = {1, 1, 2, 6, 24, 120, 720, 5040, 40320, 362880};
```

```
int use[10]:
```

```
string Kangtuo(int x) {
    CLR(use);
    clk(use);
string res = "";
for (int i = 8; ~i; i--) {
   int d = x / fac[i];
        for (int i = 0; i <= d; i++) if (use[i]) d++; res += d + '1';
        use[d] = 1;
        x %= fac[i];
    return res;
int kangtuo(string &x) {
    CLR(use); int res = 0;
    for (int i = 0; x[i]; i++) {
  int t = x[i] - '0', d = t--;
  for (int j = 1; j < d; j++) if (use[j]) t--;</pre>
        res += t * fac[8 - i];
        use[d] = 1;
    return res;
Lucas定理
11 F[MOD + 10];
void init(11 p) {
    F[0] = 1;
    for (int i = 1; i \le p; i++)
        F[i] = F[i-1]*i\% MOD;
11 inv(11 a, 11 m) {
    if (a == 1) return 1;
    return inv(m % a, m) * (m - m / a) % m;
返回C(n, m) % p
11 lucas(11 n, 11 m, 11 p)
    11 \text{ ans} = 1;
    while(n && m)
         11 a = n \% p;
        11 b = m % p;
         if (a < b) return 0;
        ans = ans * F[a] % p * inv(F[b] * F[a-b] % p, p) % p;
        n \neq p;
        m /= p;
    return ans;
大素数判断以及大整数分解
map <11, 11> mp;
map <11, 11> :: iterator iter;
11 Random(11 n) {
    return ((double) rand() / RAND MAX * n + 0.5);
11 q_mul(11 a, 11 b, 11 mod) {
    11 \text{ ans} = 0;
    while(b) {
         if(b \& 1) ans = (a + ans) \% mod;
        b >>= 1;
        a = (a + a) \% mod;
    return ans;
11 q_pow(11 a, 11 b, 11 mod) {
    11 ret = 1;
    while(b) {
        if(b & 1) ret = q_mul(ret, a, mod);
        b >>= 1;
        a = q_mul(a, a, mod);
    return ret;
bool witness(11 a, 11 n) {
    11 d = n - 1;
    while(d % 2 == 0) d >>= 1;
    11 t = q_pow(a, d, n);
    while (d != n - 1 \&\& t != 1 \&\& t != n - 1) {
```

```
t = q_mul(t, t, n);
        d <<= 1;
    return t == n - 1 \mid \mid d \& 1;
bool Isprime(11 p, 11 n) {
    if(n == 2) return true;
    if (n < 2 \mid | ! (n \& 1)) return false;
    int cnt = 20;
    while(cnt--) {
        11 base = Random(n - 2) + 1;
        if(!witness(base, p)) return false;
    return true;
11 pollard_rho(11 n, 11 c) {
    x, y, d, i = 1, k = 2; x = \text{Random}(n - 2) + 1;
    y = x;
    while(1) {
        i++;
        x = (q_mul(x, x, n) + c) \% n;
        d = \underline{gcd(y - x, n)};
if (1 \leq d && d \leq n) return d;
        if(y = x) return n;
        if(i = k) {
            y = x;
             k <<= 1;
   }
// 分解n,c是任意传入的一个数,分解的数放在mp里面
void find(11 n, 11 c) {
    if(n == 1) return;
    if(Isprime(n, n)) {
        mp[n]++;
        return;
    11 p = n;
    while(p \geq= n)
       p = pollard_rho(p, c--);
    find(p, c);
find(n / p, c);
莫比乌斯反演
int mu[maxn];
int primes[maxn], tot = 0;
int vis[maxn];
11 sum[maxn];
void Mobius(int n) {
    mu[1] = 1;
    tot = 0;
    for(int i = 2; i \le n; i++) {
        if(!vis[i]) {
             mu[i] = -1;
             primes[tot++] = i;
        for(int j = 0; j < tot && i * primes[j] <= n; j++) {
    vis[i*primes[j]] = 1;</pre>
             if(i % primes[j] != 0) mu[i*primes[j]] = -mu[i];
             else {
                 mu[i*primes[j]] = 0;
                 break;
    for (int i = 1; i \le n; i ++) {
        sum[i] = sum[i - 1] + mu[i];
// 求 (a,b) 互质的点对数
11 solve(11 a, 11 b) {
    11 \text{ ans } = 0;
    if (a > b) swap (a, b);
    for (11 i = 1, 1a = 0; i \le a; i = 1a + 1) {
        la = min(a / (a / i), b / (b / i));
        ans += (11) (sum[1a] - sum[i - 1]) * (a / i) * (b / i);
    return ans;
}
```

```
simpson公式 (积分)
```

```
//calc1是可以直接积分的部分,减少精度误差
double calc1(double x) {
   return a/4.0*x*x*x*x+b/3.0*x*x*x;
//f是除了直接积分部分的原函数
double f(double x)
   return c * x * log(x);//自定义函数
double simpson(double a, double b)
   double c = a + (b - a) / 2;
   return (f(a) + 4 * f(c) + f(b)) * (b - a) / 6;
//递归过程,可以保存la,rb,和simpson的值,若la,rb未变
//则直接使用保存的simpson值不用再调用simpson函数,
//若改变则调用函数并保存修改后的值
//eps为自定义精度
double asr (double a, double b, double eps, double A)
   double c = a + (b - a) / 2;
   double L = simpson(a, c), R = simpson(c, b);
   if (abs(L + R - A) \le 15 * eps) return L + R + (L + R - A) / 15.0;
   return asr(a, c, eps/2, L) + asr(c, b, eps/2, R);
//调用此函数
double asr main (double a, double b, double eps)
   return asr(a, b, eps, simpson(a,b));
线性规划
// 改进单纯性法的实现
// 参考: http://en.wikipedia.org/wiki/Simplex_algorithm
// 输入矩阵a描述线性规划的标准形式。a为m+1行n+1列,其中行0~m-1为不等式,行m为目标函数(最大化)。列0~n-1为变量0~n-1的系数,列n为常数项
// 第i个约束为a[i][0]*x[0] + a[i][1]*x[1] + ... <= a[i][n]
// 目标为max(a[m][0]*x[0] + a[m][1]*x[1] + ... + a[m][n-1]*x[n-1] - a[m][n])
// 注意: 变量均有非负约束x[i] >= 0
const int maxm = 500; // 约束数目上限
const int maxn = 500; // 变量数目上限
const double INF = 1e100;
const double eps = 1e-10;
struct Simplex {
 int n; // 变量个数
 int m; // 约束个数
 double a[maxm][maxn]; // 输入矩阵
 int B[maxm], N[maxn]; // 算法辅助变量
 void pivot(int r, int c) {
   swap(N[c], B[r]);
   a[r][c] = 1 / a[r][c];
   for(int j = 0; j \le n; j++) if(j != c) a[r][j] *= a[r][c];
   for (int i = 0; i \le m; i++) if (i != r) {
     for(int j = 0; j \le n; j++) if(j != c) a[i][j] -= a[i][c] * a[r][j];
     a[i][c] = -a[i][c] * a[r][c];
 bool feasible() \{
   for(;;) {
     int r, c;
     double p = INF;
     for(int i = 0; i < m; i++) if(a[i][n] < p) p = a[r = i][n];
     if(p > -eps) return true;
     p = 0;
     for (int i = 0; i < n; i++) if (a[r][i] < p) p = a[r][c = i];
     if(p > -eps) return false;
     p = a[r][n] / a[r][c];
     for(int i = r+1; i < m; i++) if(a[i][c] > eps) {
  double v = a[i][n] / a[i][c];
       if(v < p) \{ r = i; p = v; \}
     pivot(r, c);
 }
 // 解有界返回1, 无解返回0, 无界返回-1。b[i]为x[i]的值, ret为目标函数的值
 int simplex(int n, int m, double x[maxn], double& ret) {
```

```
this \rightarrow m = m;
    for (int i = 0; i < n; i++) N[i] = i;
    for (int i = 0; i < m; i++) B[i] = n+i;
     if(!feasible()) return 0;
    for(;;) {
       int r, c;
       double p = 0;
       for (int i = 0; i < n; i++) if (a[m][i] > p) p = a[m][c = i];
       if(p < eps) {
         for (int i = 0; i < n; i++) if (N[i] < n) x[N[i]] = 0; for (int i = 0; i < m; i++) if (B[i] < n) x[B[i]] = a[i][n];
         ret = -a[m][n];
         return 1;
       p = INF;
       for(int i = 0; i < m; i++) if(a[i][c] > eps) {
         double v = a[i][n] / a[i][c];
if(v < p) { r = i; p = v; }
       if (p == INF) return -1;
       pivot(r, c);
  }
/////////////// 题目相关
#include<cmath>
Simplex solver;
int main() {
  int n, m;
  while(scanf("%d%d", &n, &m) == 2) {
  for(int i = 0; i < n; i++) scanf("%lf", &solver.a[m][i]); // 目标函数
  solver.a[m][n] = 0; // 目标函数常数项
    for(int i = 0; i < m; i++)
       for(int j = 0; j < n+1; j++)
scanf("%lf", &solver.a[i][j]);
    double ans, x[maxn];
    assert(solver.simplex(n, m, x, ans) == 1);
    ans *= m;
    printf("Nasa can spend %d taka.\n", (int)floor(ans + 1 - eps));
  return 0;
```