JOURNAL OF COMBINATORIAL THEORY, Series B 54, 189–195 (1992)

Switching Reconstruction and Diophantine Equations

I. KRASIKOV AND Y. RODITTY

School of Mathematical Sciences, Tel-Aviv University, Israel

Communicated by the Editors

Received December 19, 1989

Based on a result of R. P. Stanley (*J. Combin. Theory Ser. B* **38**, 1985, 132–138) we show that for each $s \geqslant 4$ there exists an integer N_s such that any graph with $n > N_s$ vertices is reconstructible from the multiset of graphs obtained by switching of vertex subsets with s vertices, provided $n \neq 0 \pmod 4$ if s is odd. We also establish an analog of P. J. Kelly's lemma (*Pacific J. Math.*, 1957, 961–968) for the above s-switching reconstruction problem.

1. INTRODUCTION

Let $G = G(V, E)$ be a graph. Given a subset $W \subseteq V$, *the switching* G_W *of* G *at* W is the graph obtained from G by replacing all edges between W and $V \backslash W$ by the nonedges. The multiset of unlabelled graphs $D_s(G) = \{G_W : |W| = s\}$ is called *the s-switching deck* of G. A graph G is called *s-switching reconstructible* if it is uniquely defined, up to isomorphism, by $D_s(G)$.

A question concerning s-switching reconstruction of graphs was proposed by Stanley, who established the following result [11]:

THEOREM 1. *Suppose that the Krawtchouck polynomial*

$$K_s^n(x) = \sum_{i=0}^{s} (-1)^i \binom{x}{i} \binom{n-x}{s-i} \tag{1}$$

has no even integer roots in the interval $[0, n]$. *Then any graph with n vertices is s-switching reconstructible.*

Other, probably equivalent conditions, were given in [4] (for sufficient conditions of different types see [4, 5]).

0095-8956/92 $3.00

For $s \leqslant 3$ a direct calculation of the Krawtchouck polynomials [11] yields that a graph is reconstructible if

$s=1$ and $n \neq 0 \pmod 4$;

$s=2$ and $n \neq t^2$, where $t=0, 1 \pmod 4$;

$s=3$ and $n \neq 0 \pmod 4$, $n \neq (t^2+2)/3$, where $t=1, 2, 5, 10 \pmod{12}$.

Note that t can be also negative.

It turned out that for $s \geqslant 4$ the situation is quite different. Namely, we show that for any fixed $s \geqslant 4$ and $n \neq 0 \pmod 4$ if s odd, then for all sufficiently large n the corresponding Krawtchouck polynomial has no integer roots. Thus, for each fixed $s \geqslant 4$ and $s \neq 0 \pmod 4$ if s odd, all but maybe a finite number of graphs are s-vertex switching reconstructible (Theorem 4).

Our proof is based on the two following theorems on diophantine equations:

THEOREM 2 [10]. *The equation with integer coefficients*

$$y^2 = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

has only finitely many integer solutions if the RHS has at least three different roots over C, where C is the complex field.

THEOREM 3 [2, 8]. *Let $Z[X, Y]$ be the set of polynomials in two variables with integer coefficients. If $f \in Z[X, Y]$ is an irreducible binary form of degree at least three and $g \in Z[X, Y]$ has degree less than the degree of f then $f(x, y) = g(x, y)$ has only finitely many integer solutions.*

Note that Theorem 3 is ineffective whenever an effective version of Theorem 2 was established by Baker [1], although, as far as we know, these bounds are too large to solve completely diophantine equations arising in this paper (further information can be found in [9]).

Since Theorem 1 provides only a partial answer to the switching reconstruction problem one can look for parameters of a graph which are defined by $D_s(G)$. For $s=1$ some results in this direction can be found in [4, 5]. Here we establish an analog of Kelly's Lemma [3] for s-switching reconstruction. Namely, we show that the number of induced subgraphs isomorphic to a given graph H on m vertices is s-vertex switching reconstructible if $\binom{n-m}{s} + \binom{n-m}{s-m} > (1/2)\binom{n}{s}$ (Theorem 5). A stronger result will be given for $m=2$ and 3 (Theorem 6).

2. Proofs

THEOREM 4 (Main Theorem). *A graph with n vertices is s-vertex switching reconstructible if*

(i) $s=1$ *and* $n \neq 0 \pmod 4$;

(ii) $s=2$ *and* $n \neq t^2$, *where* $t=0, 1 \pmod 4$;

(iii) $s=3$ *and* $n \neq 0 \pmod 4$, $n \neq (t^2+2)/3$, *where* $t=1, 2, 5, 10 \pmod{12}$.

Moreover, for each $s \geqslant 4$ there exists an integer N_s such that a graph is s-switching reconstructible provided

(iv) $n > N_s$, *for s even,*

(v) $n > N_s$ *and* $s \neq 0 \pmod 4$, *for s odd.*

Proof. Throughout the proof we set $P_s^n(y) = K_s^n((n-y)/2)$. Thus, x is even iff $y = n \pmod 4$. Note that for the cases $s=4$ and $s=5$ the proof is based on Theorem 2, whenever for $s \geqslant 6$ we use Theorem 3.

Case $s<4$. Suppose that G is not reconstructible. By Theorem 1, for $s=1$ we have, $P_1^n(y) = y = 0$, hence $n = 0 \pmod 4$.

For $s=2$ we have $P_2^n(y) = (1/2)(y^2 - n) = 0$. Since $n = y = y^2 \pmod 4$ then $y = 0, 1 \pmod 4$ and (ii) follows.

For $s=3$ we have $P_3^n(y) = (y/6)(y^2 - 3n + 2)$, hence $n = (y^2+2)/3$ and $y = 1, 2 \pmod 3$. Now, $y^2 = 3n - 2 = 3y - 2 \pmod 4$, hence $y = 1, 2 \pmod 4$ and so, $y = 1, 2, 5, 10 \pmod{12}$.

Case $s=4$. For $s=4$ the Krawtchouck polynomial just is

$$P_4^n(y) = \frac{1}{4!}(3n^2 - 6n(y^2+1) + y^4 + 8y^2),$$

and has exactly four different roots for any integer n. Hence $P_4^n(y) = 0$ yields

$$n = y^2 + 1 \pm \left(\frac{6y^4 - 6y^2 + 9}{9}\right)^{1/2}.$$

Thus $6y^4 - 6y^2 + 9 = z^2$ for some integer z. But, by Theorem 2, this equation has only finitely many solutions, hence, by Theorem 1, all but a finite number of graphs are reconstructible from D_4.

Case $s=5$.

$$P_5^n(y) = \frac{y}{5!}(15n^2 - 10n(y^2+5) + y^4 + 20y^2 + 24),$$

and the second factor again has four different roots. Thus, either $y=0$ and, by Theorem 1, $n=0 \pmod 4$, or

$$n=\frac{y^2+5}{3}\pm\frac{(10y^4-50y^2+265)^{1/2}}{15}.$$

In the last case $(10y^4-50y^2+265)^{1/2}$ must be an integer. But, by Theorem 2, there are only finitely many such y's.

Case $s\geqslant 6$. It is known (see, e.g., [6]) that the Krawtchouck polynomials satisfy the following recurrence relation

$$\begin{gathered}(s+1)P^n_{s+1}(y)=yP^n_s(y)-(n-s+1)P^n_{s-1}(y),\\ P^n_0(y)=1, \qquad P^n_1(y)=y.\end{gathered} \tag{2}$$

Putting $z=y^2$ and using induction on s one obtains

$$\begin{gathered}P^n_{2s}(y)=f_{2s}(z,n)+g_{2s}(z,n)\\ P^n_{2s+1}(y)=z^{1/2}(f_{2s+1}(z,n)+g_{2s+1}(z,n)),\end{gathered} \tag{3}$$

where $f_i(z,n)$ is a binary form of degree $\lfloor i/2\rfloor$ and $g_i(z,n)$ is a polynomial of degree less than that of $f_i(z,n)$. Indeed, since $P^n_s(y)=(1/s!)(y^s+a_1(n)y^{s-1}+\cdots+a_s(n))$ has degree exactly s then $f_s(z,n)$ is not identically zero. Rewritting (2) as

$$(s+1)P^n_{s+1}(y)=(yP^n_s(y)-nP^n_{s-1}(y))+(s-1)P^n_{s-1}(y)$$

and using the induction hypothesis we convince that the first term in the RHS is a binary form of degree $\lfloor i/2\rfloor$ plus a polynomial of degree less than $\lfloor i/2\rfloor$, whenever the second term is a polynomial of degree less than $\lfloor i/2\rfloor$.

Thus, in view of Theorem 3, it is enough to show that $f_{2s}(z,n)$ is irreducible.

For set $Q_{2s}(z,n)=(2s)!f_{2s}(z,n)$, $Q_{2s+1}(z,n)=(2s+1)!\,z^{1/2}f_{2s+1}(z,n)$. Then, by (2) and (3), $Q_i(z,n)$ satisfy the recurrence relation

$$\begin{gathered}Q_{s+1}(z,n)=z^{1/2}Q_s(z,n)-nsQ_{s-1}(z,n),\\ Q_0(z,n)=1, \qquad Q_1(z,n)=z^{1/2}.\end{gathered} \tag{4}$$

By induction on s one easily gets

$$\begin{gathered}Q_{2s}(z,n)=\sum_{i=0}^{s} az^{s-i}n^i=\sum_{i=0}^{s}(-1)^i\binom{2s}{2i}(2i-1)!!\,z^{s-i}n^i\\ Q_{2s+1}(z,n)=z^{1/2}\sum_{i=0}^{s} b_iz^{s-i}n^i=z^{1/2}\sum_{i=0}^{s}(-1)^i\binom{2s+1}{2i}(2i-1)!!\,z^{s-i}n^i,\end{gathered} \tag{5}$$

where $(2m-1)!!=\prod_{j=1}^{m}(2j-1)$, $(-1)!!=1$.

Let now p be the largest prime less than $2s$. Then $a_0 = 1$, $a_s = (2s-1)!!$ and so, $p \nmid a_0$, $p^2 \mid a_s$. On the other hand, if $2i-1 \geqslant p$ then $p \mid (2i-1)!!$, hence $p \mid a_i$. If $2i-1 < p$ then $p \mid \binom{2s}{2i}$, hence, again $p \mid a_i$. Thus, $Q_{2s}(z, n)$ is irreducible by Eisenstein criterion (see, e.g., [12, p. 161]), and hence, the theorem is proved s even.

Similarly, for s odd $z^{-1/2}Q_s(z, n)$ is also irreducible. Thus, for sufficiently large n the only integer root of P_s^n arises from $z = 0$. Then $n - 2x = 0$ and, by Theorem 1, for a non-reconstructible graph we get $n = 0 \pmod 4$. Hence the proof is completed. ▌

Remark 1. For $s = 4$ and $n \leqslant 10^8$ the polynomial $P_4^n(x)$ has an even root in the interval $[0, n]$ only for $n = 17, 66, 1521, 15043$.

For $s = 5$ and $n \leqslant 10^8$ the corresponding exceptional values of $n, n \neq 0 \pmod 4$, are 17, 67, 289, 10882.

A question of whether 15043 is sufficiently large remains open.

THEOREM 5. *Let $\mu(H \to G)$ be the number of subgraphs of G isomorphic to H. Then $\mu(H \to G)$ is reconstructible from $D_s(G)$, provided $\binom{n-m}{s} + \binom{n-m}{s-m} > (1/2)\binom{n}{s}$, where $m = |V(H)|$ and $\binom{a}{b} = 0$ if $a < b$ or $b < 0$.*

Proof. A switching G_W with $|W| = k$ will be called a k-switching. Given a graph G, $|V(G)| = n$, and integers s, m satisfying

$$\binom{n-m}{s} + \binom{n-m}{s-m} > \frac{1}{2}\binom{n}{s}. \tag{6}$$

Let $L_m = \{H^1, H^2, ...\}$ be the set of all unlabelled graphs on m vertices. Let $A_k^m(ij)$ be a matrix whose rows and colomn are indexed by elements of L_m and the entries $a_{ij} = |\{W \subseteq V(H^j) : H^j_W \simeq H^i, |W| = k\}|$. Note that $A_0^m = A_m^m$ is a unite matrix, since a switching of an empty set as well as of the whole set of vertices is the identity.

Consider the matrix $B = B_s^m = \sum_{k=0}^m \binom{n-m}{s-k} A_k^m$. Observe that any colomn sum of A_k^m is $\binom{m}{k}$, hence, for column sums of B we have

$$\sum_{k=0}^{m} \binom{n-m}{s-k}\binom{m}{k} = \binom{n}{s}.$$

Moreover, each diagonal element b_{ii} of B is at least $\binom{n-m}{s} + \binom{n-m}{s-m}$, the contribution of $\binom{n-m}{s}A_0^m + \binom{n-m}{s-m}A_m^m$ in B. Hence, by (6), $b_{ii} > \sum_{j \neq i} a_{ji}$ and thus, B is invertible.

Now, define a vector $\mu_m(G) = \mu(G) = (\mu_1, \mu_2, ...)$ where $\mu_i = \mu(H^i \to G)$. We also set $\mu(D_s(G)) = \sum_{F \in D_s(G)} \mu(F)$.

Fix $F \subset G$, $|V(F)| = m$ and $Z \subset V(F)$, $|Z| = k$. Consider an s-switching G_W such that $W \cap V(F) = Z$. There are $\binom{n-m}{s-k}$ possible choices of such a W

each of which transforms F into F_Z. Therefore, the lth component of the vector $\binom{n-m}{s-k}A_k^m\mu(G)$ is just the number of subgraphs isomorphic to H^l in $D_s(G)$ which were obtained by a k-switching of the m vertices subgraphs of G. Therefore we have the equation $B\,\mu(G)=\mu(D_s(G))$.

Here the RHS is known, the matrix B is invertible and so, one can find $\mu(G)$. ∎

For $m=2$, i.e., when H is a single edge, and $m=3$ we will show a little more, namely,

THEOREM 6. *If $m=2,3$ then $\mu(H\to G)$ is reconstructible from $D_s(G)$ except, possibly, the cases $s=\binom{t}{2}$ and $n=t^2$ or $n=(t-1)^2$, $t=2,3,\ldots$.*

Proof. For $m=2$ or 3 the matrix B_s^m can be easily calculated, namely,

$$A_1^2=\begin{pmatrix}0&2\\2&0\end{pmatrix},\qquad B_s^2=\begin{pmatrix}a&2b\\2b&a\end{pmatrix},$$

$$A_1^3=A_2^3=\begin{pmatrix}0&0&1&0\\0&2&0&3\\3&0&2&0\\0&1&0&0\end{pmatrix},\qquad B_s^3=\begin{pmatrix}c&0&d&0\\0&c+2d&0&3d\\3d&0&c+2d&0\\0&d&0&c\end{pmatrix},$$

where

$$a=\binom{n-2}{s}+\binom{n-2}{s-2},\qquad b=\binom{n-2}{s-1},$$

$$c=\binom{n-3}{s}+\binom{n-3}{s-3},\qquad d=\binom{n-3}{s-1}+\binom{n-3}{s-2},$$

and the graphs are listed by increasing the number of edges.

Hence, $\det B_s^2=(a-2b)(a+2b)$, $\det B_s^3=(a+3b)^2(a-b)^2$. One can see that in both cases B is not invertible only if $s=\binom{t}{2}$ and $n=t^2$, $t=2,3,\ldots$. We omit the details. ∎

Remark 2. One can check that the matrices A_k^m satisfy the recurrence

$$(k+1)A_{k+1}^m=(k+1)A_k^mA_1^m-(m-k+1)A_{k-1}^m, \tag{7}$$

i.e., precisely the recurrence (2) for the Krawtchouck polynomials. Indeed, the entry ij of $A_k^mA_1^m$ is just the number of ways to obtain H^i from H^j by a two-steps switching: first k vertices and then one vertex. Thus, the result will be either $(k+1)$- or $(k-1)$-switching, and in the first case we have $(k+1)$ choices for the first step, while in the second case there are $(n-k+1)$ choices.

This observation shows that B_s^m is invertible iff no eigenvalue of A_1^m is the root of the polynomial

$$R_k^m(y) = \sum_{k=0}^{m} \binom{n-m}{s-k} P_k^m(y).$$

Remark 3. Note that two graphs are not s-switching reconstructible iff the corresponding columns of A_s^n are equal. It easily follows from (7) and (3) that $A_{2s+1}^n = A_1^n C$ for some matrix C. Hence, if A_1^n has two equal columns then A_{2s+1}^n has two also. Thus if G is not 1-switching reconstructible then it is not $(2s+1)$-switching reconstructible for all s.

It is natural to ask whether the degree sequence of a graph is reconstructible? Stanley proved that the answer is "yes" for $s=1$ and $n \neq 4$ [11]. As far as we know, the question remains open even for $s=2$.

In conclusion let us formulate the following conjecture which can be considered as an analog of the Nah-Williams Lemma [7] for the 1-switching reconstruction problem:

Conjecture. Let $D_1(G) = D_1(H)$ but $G \not\simeq H$, then there is a pairing $(v, \sigma(v))$, $v \neq \sigma(v)$, of the vertices of G such that the switching of any t pairs results in H for t odd and in G for t even.

REFERENCES

1. A. BAKER, Bounds for the solution of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.* **65** (1969), 439-444.
2. H. DAVENPORT AND D. J. LEWIS, unpublished.
3. P. J. KELLY, A congruence theorem for trees, *Pacific J. Math.* (1957), 961–968.
4. I. KRASIKOV AND Y. RODITTY, Balance equations for reconstruction problems, *Arch. der Math.* **48** (1987), 458–464.
5. I. KRASIKOV, A note on the vertex switching reconstruction, *Internat. J. Math. Math. Sci.* **11**, No. 4 (1988), 825–827.
6. J. H. VAN LINT, "Introduction to Coding Theory," Springer-Verlag, New York/Berlin, 1982.
7. C. ST. J. A. NASH-WILLIAMS, The reconstruction problem, *in* "Selected Topics in Graph Theory" (L. W. Beinike and R. J. Wilson, Eds.) pp. 205–236, Academic Press, San Diego, 1978.
8. A. SCHINZEL, An improvement of Runge's theorem on diophantine equations, *Comment. Pontific. Acad. Sci.* **2**, No. 20 (1969), 9.
9. T. H. SHORY AND R. TIJEMAN, "Exponential Diophantine Equations," Cambridge Univ. Press, London/New York, 1986.
10. C. L. SIEGEL, The integer solution of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$, *J. London Math. Soc.* **1** (1920), 66–68.
11. R. P. STANLEY, Reconstruction from vertex switching, *J. Combin. Theory Ser. B* **38** (1985), 132–138.
12. ROBERT C. TOMPSON AND ADIL YAQUB, "Introduction to Abstract Algebra," Scott, Foresman, Glenview, IL, 1970.