THE DISTANCE OF A PERMUTATION FROM A SUBGROUP OF S_n

RICHARD G.E. PINCH

For Bela Bollobas on his 60th birthday

Abstract. We show that the problem of computing the distance of a given permutation from a subgroup H of S_n is in general NP-complete, even under the restriction that H is elementary Abelian of exponent 2. The problem is shown to be polynomial-time equivalent to a problem related to finding a maximal partition of the edges of an Eulerian directed graph into cycles and this problem is in turn equivalent to the standard NP-complete problem of Boolean satisfiability.

1. Introduction

We show that the problem of computing the distance of a given permutation from a subgroup H of S_n is in general NP-complete, even under the restriction that H is elementary Abelian of exponent 2. The problem is polynomial-time equivalent to finding a maximal partition of the edges of an Eulerian directed graph into cycles and this is turn equivalent to the standard NP-complete problem **3-SAT**.

2. Distance in the symmetric group

We define *Cayley distance* in a symmetric group as the minimum number of transpositions which are needed to change one permutation to another by post-multiplication

$$d(\rho,\pi) = \min\{n \mid \rho\tau_1 \ldots \tau_n = \pi, \quad \tau_i \text{ transpositions }\}.$$

It is well-known that Cayley distance is a metric on S_n and that it is homogeneous, that is, $d(\rho,\pi) = d\left(I, \rho^{-1}\pi\right)$. Further, the distance of a permutation π from the identity in S_n is n minus the number of cycles in π.

If H is a subgroup of S_n, then we define the distance of a permutation π from H as

$$d(H,\pi) = \min_{\eta \in H} d(\eta,\pi).$$

We refer to Critchlow [2] and Diaconis [3] for background and further material on the uses of the Cayley and other metrics on S_n.

Problem 1 (Subgroup–Distance)**.** Instance: *Symmetric group S_n, element $\pi \in S_n$, elements $\{h_1,\ldots,h_r\}$ of S_n, integer K.*
Question: *Is there an element $\eta \in H = \langle h_1,\ldots,h_r\rangle$ such that $d(\eta,\pi) \le K$?*

The natural measure of this problem is nr where r is the length of the list of generators. The following result shows that every subgroup of S_n has a set of generators of length at most n^2 and hence we are justified in taking n as the measure of the various problems derived from **Subgroup–Distance**.

Proposition 1. *Every subgroup of S_n can be generated by at most n^2 elements.*

Date: 20 November 2005.
1991 *Mathematics Subject Classification.* Primary 20B40; Secondary 05C38, 20B35, 68Q25.

Proof. Let H be a subgroup of S_n. It is clear that H is generated by the union of one Sylow subgroup for every prime p dividing the order $\#H$. The order of a Sylow p-subgroup of H is p^b where p^b divides $\#H$ and hence $n!$. It is well-known (e.g. Dickson [4] I, chap 9) that the power of p dividing $n!$ is at most $\frac{n}{p-1}$, so $b \le n$. But consideration of the composition factors shows that a p-group of order p^b can be generated by a set of at most b elements: hence any Sylow subgroup of H can be generated by at most n elements. Further, the set of prime factors of the order of H forms a subset of the set of prime factors of $n!$, that is, of the primes up to n, and there are at most n such primes. Hence H can be generated by a set of at most n^2 elements.

□

Although we do not need the stronger result, it can be shown that any subgroup of S_n can be generated by at most $3n-2$ elements.

We define a subset of S_n to be *involutions with disjoint support (IDS)* to be set of elements of the form $\gamma_j = \left(x_j^{(1)}\, y_j^{(1)}\right) \dots \left(x_j^{(r_j)}\, y_j^{(r_j)}\right)$ where the $x_j^{(i)}, y_j^{(i)}$ are all distinct. The subgroup generated by an IDS is clearly elementary Abelian with exponent 2. Define the *width* of an IDS to be the maximum number of 2-cycles r_j in the generators γ_j. The problem **IDS**w**–Subgroup–Distance** is the problem **Subgroup–Distance** with the list of generators restricted to be an IDS of width at most w.

Theorem 2. *The problem* **IDS6–Subgroup–Distance** *is NP-complete.*

The Theorem will follow from combining Theorem 3 and Theorem 7. We deduce immediately that the more general problem **Subgroup–Distance** is also NP-complete.

By contrast, the problem of deciding whether the distance is zero, that is, testing for membership of a subgroup of S_n, has a polynomial-time solution, an algorithm first given by Sims [8] and shown to have a polynomial-time variant by Furst, Hopcroft and Luks [5]. See Babai, Luks and Seress [1] and Kantor and Luks [7] for a survey of related results.

3. Switching circuits

Let $G = (V, E)$ be a directed graph with vertex set V and edge set E. (We allow loops and multiple edges.) For each vertex v define $e_+(v)$ to be the set of edges out of v and $e_-(v)$ the set of edges into v. The in-valency $\partial_-(v) = \#e_-(v)$ and the out-valency $\partial_+(v) = \#e_+(v)$. We define a *switching circuit* to be a directed graph G for which $\partial_+(v) = \partial_-(v) = \partial(v)$, say, and for which there is a labelling $l_\pm(v)$ of each set $e_\pm(v)$ with the integers from 1 to $\partial(v)$. (The labels at each end of an edge are not related.) A *routing* ρ for a switching circuit is a choice of permutation $\rho(v) \in S_{\partial(v)}$ for each vertex v. Clearly there is a correspondence between routings for a switching circuit G and decompositions of the edge set of G into directed cycles. We define a *polarisation* T for a switching circuit G to be an equivalence relation on the set of vertices such that equivalent vertices have the same valency, and call (G, T) a *polarised switching circuit.* We say that a routing ρ *respects* the polarisation T if the permutations $\rho(x)$ and $\rho(y)$ are equal whenever x and y are equivalent vertices under T. We shall sometimes refer to a switching circuit without a polarisation, or with a polarisation for which all the classes are trivial, as *unpolarised.*

Problem 2 (Polarised–Switching–Circuit–Maximal–Routing)**.** Instance: *Polarised switching circuit* (G, T)*, positive integer* K*.*
Question: *Is there a routing which respects* T *and has at least* K *cycles in the associated edge-set decomposition?*

We define the *width* of a polarisation to be the maximum number of vertices in an equivalence class of T. The problem **Width**w–**Valency**v–**Maximal–Routing** is the problem **Polarised–Switching–Circuit–Maximal–Routing** with the width of T constrained to be at most w and the in- and out-valency of each vertex in V constrained to be at most v.

Theorem 3. *Problem* **Width**6–**Valency**2–**Maximal–Routing** *is NP-complete.*

4. Proof of Theorem 3

We shall show that the problem **3-SAT**, [LO2] of Garey and Johnson [6], which is known to be NP-complete, can be reduced to the problem **Width**6–**Valency**2–**Maximal–Routing**.

We define a polarised switching circuit (G, T) to be *Boolean* (or *binary*) if every vertex has in- and out-valency 1 or 2. To each class C of the polarisation T we associate a Boolean variable $a(C)$. There is then a 1-1 correspondence between routings ρ which respect T and assignments of truth values to the variables $a(C), C \in T$ by specifying that $a(C)$ is 0 (false) if and only if the permutation $\rho(v)$ is the identity in S_2 for every v in C, and 1 (true) if and only if $\rho(v) = (1\,2)$.

We denote a vertex in a polarisation class associated with the Boolean variable a as in Figure 1. Out convention for drawing the diagrams will be to assume the edges round each vertex labelled so that 1 is denoted by either "straight through" or "turn right".

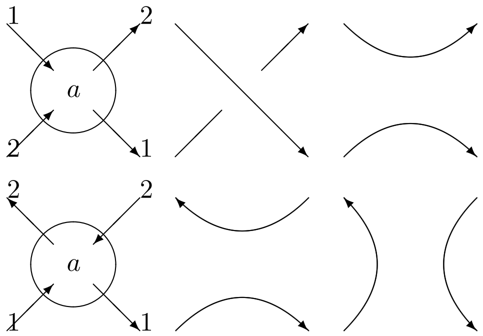

Figure 1. A vertex in a switching circuit associated with the Boolean variable a, and the routings with $a = 1$ and $a = 0$ respectively

We associate a vertex with the negated variable $\bar{a}$ by exchanging the input labels 1 and 2.

Our proof will proceed by finding polarised switching circuits for which the number of maximal cycles in a routing is a Boolean function of the variables.

For a single Boolean variable a define $I(a)$ to be the switching circuit in Figure 2.

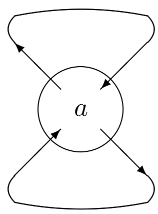

Figure 2. The switching circuit $I(a)$.

For a pair of Boolean variables (a, b) define the polarised switching circuit $E(a, b)$ as in Figure 3.

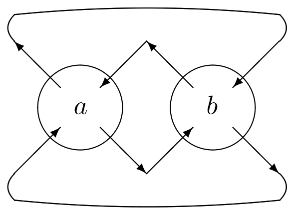

FIGURE 3. The switching circuit $E(a, b)$.

Further define the polarised switching circuit $F(a, b)$ as in Figure 4.

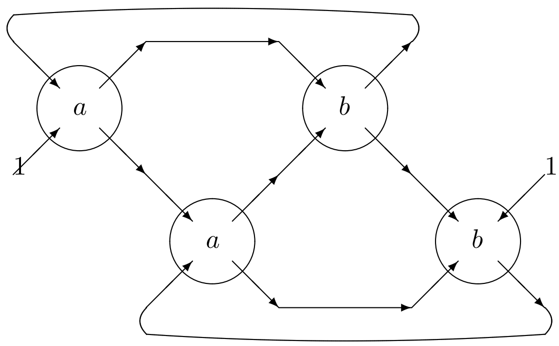

FIGURE 4. The switching circuit $F(a, b)$.

Define $G(a, b)$ to be the disjoint union of $F(a, b)$ and $E(\bar{a}, b)$.

Proposition 4. (1) *The number of cycles in a routing for $I(a)$ is 2 if $a = 1$ and otherwise 1.*
(2) *The number of cycles in a routing for $E(a, b)$ is 2 if $a = b$ and otherwise 1.*
(3) *The number of cycles in a routing for $F(a, b)$ is 2 if $a \neq b$, 3 if $a = b = 1$ and 1 if $a = b = 0$.*
(4) *The number of cycles in a routing for $G(a, b)$ is 2 if $a = b = 0$ and 4 otherwise.*

Proof. In each case we simply enumerate the cases.

□

For a triple of Boolean variables (a, b, c) define the polarised switching circuit $A(a, b, c)$ as in Figure 5.

Proposition 5. *The number of cycles in a routing for $A(a, b, c)$ is 1 if $a = b = c = 0$ and 3 otherwise.*

Proof. Again, in each case we simply enumerate the cases.

□

Theorem 6. *There is a polynomial-time parsimonious transformation from the problem* **3-SAT** *to the problem* **Width6–Valency2–Maximal–Routing**.

Proof. Suppose we have an instance of **3-SAT**: that is, a Boolean formula Φ of length l in variables x_i which is a conjunct of k clauses each of which is a disjunct of at most three variables (possibly negated). We transform Φ into a formula Φ' in variables y_i^j by replacing the j^{th} occurence of variable x_i by the variable y_i^j and

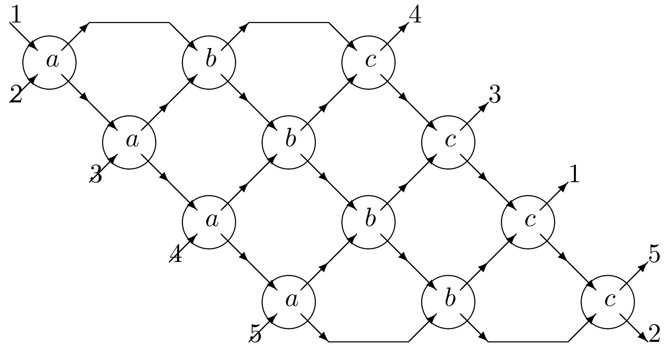

FIGURE 5. The switching circuit $A(a, b, c)$.

conjoining clauses $\left(y_i^1 \equiv y_i^2\right) \wedge \ldots \wedge \left(y_i^{(r_i-1)} \equiv y_i^{(r_i)}\right)$ where the variable x_i occurs r_i times in Φ. Clearly Φ and Φ' represent the same Boolean function and have the same number of satisfying assignments. Every variable in Φ' occurs at most three times, and at most once in a disjunct deriving from a clause in Φ. Let n be the total number of variables in Φ'; certainly $n \le l$.

We form a polarised switching circuit Ψ from Φ' as follows. Take a circuit $B(x, y, z)$ for every clause in Φ' of the form $(x \vee y \vee z)$; take a circuit $G(x, y)$ for every clause in Φ' of the form $(x \vee y)$; take a circuit $I(x)$ for every clause in Φ' of the form (x); take a circuit $E(x, y)$ for every clause in Φ' of the form $(x \equiv y)$. Let the number of circuits of types B, G, I and E taken to form Ψ be b, g, i, and e respectively. Put $M = 3b + 4g + 2i + 2e$. The resulting polarised switching circuit has n classes, and each class in the polarisation is involved in at most one circuit of the form B, G or I: hence each class contains at most $4+1+1 = 6$ vertices and the number of vertices in Ψ is thus at most $6n$. Furthermore, a routing for Ψ has M cycles if and only if the corresponding assignment of Boolean values gives Φ', and hence Φ, the value 1; otherwise a routing has less than M cycles.

□

Since the problem **3-SAT** is known to be NP-complete, we immediately deduce that the problem **Width**16–**Valency**2–**Maximal**–**Routing** is NP-complete as well. This proves Theorem 3.

5. SWITCHING CIRCUITS AND IDS

In this section we obtain a polynomial-time equivalence between the problems **Width**w–**Valency**2–**Maximal**–**Routing** and **IDS**w–**Subgroup**–**Distance**.

Theorem 7. *There is a polynomial-time parsimonious equivalence between problems* **Width**w–**Valency**2–**Maximal**–**Routing** *and* **IDS**w–**Subgroup**–**Distance**.

Proof. Suppose we have an instance of **IDS**w–**Subgroup**–**Distance**, that is, an element π of S_n together with an IDS on a set of t generators $\{\gamma_j\}$ with $\gamma_j = \left(x_j^{(1)}\, y_j^{(1)}\right) \ldots \left(x_j^{(r_j)}\, y_j^{(r_j)}\right)$, the $x_j^{(i)}, y_j^{(i)}$ all distinct and all the $r_j \le w$. We construct a polarised switching circuit on a graph, vertex set $V = \{P(1), \ldots, P(n)\} \cup \{Q(1, 1), \ldots, Q(t, r_t)\}$. Each vertex $P(k)$ will be of in-valence and out-valence 1; each vertex $Q(j, i)$ will be of in-valence and out-valence 2. For each j up to t and i up to r_j we take edges from $P(x_j^i)$ and from $P(y_j^i)$ to $Q(j, i)$ labelled 1 and 2 respectively, and edges from $Q(j, i)$ to $P\left(\pi\left(x_j^i\right)\right)$ and to $P\left(\pi\left(y_j^i\right)\right)$ again labelled 1 and 2 respectively. We define a polarisation T on V by taking t classes $C_j = \{Q(j, i) \mid i = 1, \ldots, r_j\}$; clearly the width of T is at most w.

Conversely, suppose we have an instance of **Width**w**–Valency**2**–Maximal–Routing**, that is, a directed graph (V,E) with every vertex v having in- and out-valency two, a labelling $l_{\pm}(v) : e_{\pm}(v) \to \{1,2\}$ of edges into and out of each vertex v, and an equivalence relation T on V with t classes each of size at most w. Put $n = \#E$. We define a permutation π of E as follows. For an edge e into a vertex v, let $\pi(e)$ be the edge f out of v which has label $l_+(v)(f)$ equal to $l_-(v)(e)$. We further define an IDS by writing down a set of generators $\{\gamma_j\}$ as follows. For each class of vertices $C_j = \left\{ v_i^j \mid i = 1, \ldots, r_j \right\}$ in the polarisation T, let γ_j be the product of transpositions of the form $\left(f_i^j \, g_i^j \right)$ where f_i^j and g_i^j are the edges out of vertex v_i^j. Since each class in T has at most w elements, each generator γ_j is composed of at most w transpositions.

In each case there is a correspondence between routings ρ of the switching circuit which respect the polarisation T and permutations of the form $\pi\eta$ where η runs over the elements of the subgroup H of S_n generated by the γ_j: in this correspondence the number of cycles in the routing ρ is equal to the number of cycles in the permutation $\pi\eta$. Hence π is within distance d of the group generated by the γ_j if and only if there is a routing ρ with at least $n - d$ cycles.

□

References

[1] L. Babai, E.M. Luks, and Seress Á., *Fast management of permutation groups*, Proc. 29th annual symposium on foundation of computer science (1988), 272–282.

[2] D.E. Critchlow, *Metric methods for analysing partially ranked data*, Lecture notes in statistics, vol. 34, Springer Verlag, Berlin, 1985.

[3] P. Diaconis, *Group representations in probability and statistics*, IMS lecture notes, vol. 11, Institute of Mathematical Statistics, Hayward CA, 1988.

[4] Leonard E. Dickson, *History of the theory of numbers*, Chelsea, New York, 1971, original publication Carnegie Institute, Washington, 1919–23.

[5] M.L. Furst, J. Hopcroft, and E.M. Luks, *Polynomial time algorithms for permutation groups*, Proc. 21st IEEE FOCS, 1980, pp. 36–41.

[6] M.R. Garey and G.S. Johnson, *Computers and intractability: a guide to the theory of np-completeness*, W.H. Freeman, San Francisco, CA, 1979.

[7] W.M. Kantor and E.M. Luks, *Computing in quotient groups*, Proceedings 22nd annual ACM symposium on theory of computing, ACM Press, 1990, pp. 524–534.

[8] C.C. Sims, *Computational methods in the study of permutation groups*, Computational problems in abstract algebra (Oxford) (J. Leech, ed.), Pergamon Press, 1970, pp. 169–184.

2 Eldon Road, Cheltenham, Glos GL52 6TU, U.K.

E-mail address: rgep@chalcedon.demon.co.uk