On Minimal Factorisations of Sporadic Groups

P. E. Holmes

CONTENTS

2000 AMS Subject Classification: Primary 20D08; Secondary 94A60

Keywords: Simple groups, sporadic groups, cryptography

Minimal factorisations of groups can be used in cryptography. It is not yet known if one exists for each finite group, although it has been shown that a minimal counterexample of a group without one must be simple. We prove existence of minimal factorisations for some sporadic groups.

1. INTRODUCTION

For many years cryptographers have used large abelian finite groups but some are now turning their attention to non-abelian ones. They feel that these could be a good source of "trap doors" that can be used in public key encryption [Magliveras 02].

One proposed system is MST1 [Magliveras 02]. This uses a certain type of group factorisation to encode messages which can only be decoded by the recipient. In [Vasco et al. 03], González Vasco et al. conjecture that minimal factorisations of this type exist for all finite groups. Proofs are given in [Magliveras 02] that they exist for $\mathrm{L}_2(q)$ for any prime power q and all alternating groups A_n. In [Vasco et al. 03] it is proved that they exist for the Mathieu sporadic groups, the group $\mathrm{U}_3(3)$, and any group with a factorisation into Sylow subgroups, and hence that one exists for any group of order less than $|\mathrm{J}_1|$.

Later in this section we define minimal factorisations and related concepts. Section 2 lists some sufficient conditions for the existence of minimal factorisations. In Section 3 we prove the existence of minimal factorisations for the sporadic groups J_1, J_2, HS, $\mathrm{M^cL}$, He, and Co_3. We also show that the existence of minimal factorisations for certain smaller groups implies their existence for Ru and Suz. We draw our conclusions in Section 4.

1.1 Some Definitions

Let G be a finite group and α be a sequence $[\alpha_1, \ldots, \alpha_s]$, where each α_i is a sequence of elements of G of length r_i. Then we call α a *logarithmic signature* if every $g \in G$ can be uniquely written as a product $\beta_1 \cdots \beta_r$, with $\beta_i \in \alpha_i$.

© A K Peters, Ltd.

1058-6458/2004$ 0.50 per page

The *length* of a logarithmic signature is $\sum_{i=1}^{s} r_i$. By the definition of a logarithmic signature we have $|G| = \prod_{i=1}^{s} r_i$; so it is clear that a lower bound for the length of a logarithmic signature is $\mathcal{B}(G) = \sum_{p \in P} k_p p$ where P is the set of primes dividing $|G|$ and k_p is the highest power of p dividing $|G|$. We call a logarithmic signature whose length achieves this lower bound a *minimal factorisation* for G.

If G has a factorisation $\alpha = [\alpha_1, \dots, \alpha_s]$ where α_1 is the sequence of all elements in a subgroup H and $\sum_{i=2}^{s} r_i = \sum_{i=1}^{k} a_i p_i$ where $[G : H] = p_1^{a_1} \dots p_k^{a_k}$ then we say that G has a *minimal factorisation over* H.

2. CONDITIONS FOR EXISTENCE OF MINIMAL FACTORISATIONS

In [Vasco et al. 03], the authors give some sufficient conditions for a group G to have a minimal factorisation. One of these is listed below as Condition 2.1, while the others are embraced by Condition 2.2. We add Conditions 2.3, 2.4, 2.5, and 2.6.

Condition 2.1. *If G has a normal subgroup K with $G/K \cong H$ and H and K both have minimal factorisations, then G has a minimal factorisation.*

Condition 2.1 shows that any minimal counterexample to the conjecture that all groups have minimal factorisations must be simple. It also implies that all soluble groups have minimal factorisations.

Condition 2.2. *If G contains subgroups $H_1, \dots, H_n$ such that*

(1) $|G| = |H_1| \dots |H_n|$,

(2) *H_i has a minimal factorisation for all i, and*

(3) $G = H_1 \dots H_n$,

then G has a minimal factorisation.

Proof: Juxtaposing minimal factorisations for the H_i gives a factorisation of length $\mathcal{B}(H_1) + \dots + \mathcal{B}(H_n) = \mathcal{B}(G)$. By (3) this is a logarithmic signature for G, and therefore it is a minimal factorisation. □

Special cases of this condition were used in the proofs that minimal factorisations exist for Mathieu groups, alternating groups, and the groups $L_2(q)$. It also shows that they exist whenever G has a factorisation into its Sylow subgroups.

Condition 2.3. *A group G has a minimal factorisation if it contains two subgroups H and K with the following properties:*

(1) *$|G| = p|H||K|/|K_1|$ where p is either 4 or prime and K_1 is a subgroup of K;*

(2) *On restriction to K of the permutation representation of G on the cosets of H, the $p|K|/|K_1|$ cosets of H in G fall into p equal-sized orbits. The subgroup K_1 fixes a point inside each orbit;*

(3) *H has a minimal factorisation and K has a minimal factorisation over K_1.*

Proof: By (1), the permutation representation of G on the cosets of H is an action on $p|K|/|K_1|$ points. By (2), every orbit of K on these points has equal length, so K divides the points into p orbits each of size $|K|/|K_1|$. Because G acts transitively on the points, we can find a sequence of p elements $X = [x_1, \dots, x_p]$ mapping the fixed point of H to the fixed point of K_1 in each of the p K-orbits. So every element of G can be written uniquely as hx_ik_j for some $h \in H$ and $1 \leq i \leq p$, where k_j is one of a set of coset representatives for K_1 in K.

Let $[\alpha_1, \dots, \alpha_r]$ be a minimal factorisation for H and $[\beta_1, \dots, \beta_s]$ be a minimal factorisation for K over K_1. Consider the sequence $\gamma = [\alpha_1, \dots, \alpha_r, X, \beta_2, \dots, \beta_s]$. The previous paragraph shows that γ is a logarithmic signature for G. By (1), we have $\mathcal{B}(G) = p + \mathcal{B}(H) + \mathcal{B}(K) - \mathcal{B}(K_1)$, which is the length of γ. So γ is a minimal factorisation for G. □

Condition 2.4. *If G contains two subgroups H and K such that*

(1) *H has a minimal factorisation;*

(2) *K acts transitively in the permutation representation of G on the cosets of H;*

(3) *K has a minimal factorisation over $K \cap H$;*

then G has a minimal factorisation.

Proof: Let $[\alpha_1, \dots, \alpha_r]$ be a minimal factorisation for H and $[\beta_1, \dots, \beta_s]$ be a minimal factorisation for K over $K \cap H$. This time consider the sequence $\gamma = [\alpha_1, \dots, \alpha_r, \beta_2, \dots, \beta_s]$. The length of γ is $\mathcal{B}(H) + \mathcal{B}(K) - \mathcal{B}(K \cap H) = \mathcal{B}(G)$. By (2), a set of coset representatives for $K \cap H$ in K is also a full set of coset representatives for H in G. So γ is a minimal factorisation for G. □

Condition 2.5. *If G contains two subgroups H and K such that*

(1) *K has a subgroup K_1 which is the full point stabiliser in each orbit of K on the cosets of H;*

(2) *$|G| = pq|H||K|/|K_1|$ where p and q are either 4 or prime;*

(3) *$p \leq q$ and G is p-transitive on the cosets of H;*

(4) *H has a minimal factorisation and K has a minimal factorisation over K_1;*

then G has a minimal factorisation.

Proof: In this case K has pq orbits of equal length on the cosets of H. We find a sequence of p elements, X, mapping the fixed point of H to a set $\mathcal{P}$ of any p distinct points. We can then use the p-transitivity of G to find a sequence $Y = [y_1, \ldots, y_q]$ of q elements such that $\cup_{i=1}^{q} \mathcal{P} y_i$ contains a fixed point of K_1 in each of the pq K-orbits.

Again let $[\alpha_1, \ldots, \alpha_r]$ be a minimal factorisation for H and $[\beta_1, \ldots, \beta_s]$ be a minimal factorisation for K over K_1. Consider the sequence $\gamma = [\alpha_1, \ldots, \alpha_r, X, Y, \beta_2, \ldots, \beta_s]$. The previous paragraph shows that γ is a logarithmic signature. By (2), we have $\mathcal{B}(G) = p + q + \mathcal{B}(H) + \mathcal{B}(K) - \mathcal{B}(K_1)$, which is the length of γ. So γ is a minimal factorisation for G. □

Condition 2.6. *If G contains two subgroups H and K and there exist two sequences S and T of elements of G such that*

(1) *K has a subgroup K_1 which is the full point stabiliser in each orbit of K on the cosets of H in G;*

(2) *$|G| = pq|H||K|/|K_1|$ where p and q are either 4 or prime;*

(3) *$|S| = p$ and $|T| = q$;*

(4) *In the permutation representation of G on the cosets of H, each element of $\{st | s \in S, t \in T\}$ maps the fixed point of H to some point p_{st} that is fixed by $K \cap H$;*

(5) *Each of the pq points p_{st} is in a distinct orbit of K in this permutation representation;*

(6) *H has a minimal factorisation and K has a minimal factorisation over $K \cap H$;*

then G has a minimal factorisation.

Proof: This condition is a generalised version of Condition 2.5.

Each product of the form st with $s \in S$, $t \in T$ maps the fixed point of H into a distinct orbit of K on the cosets of H in G, so a representative of each coset of H in G can be written in the form stk for some $s \in S$, $t \in T$, and $k \in K$. As the points p_{st} are all fixed by $K \cap H$, we can replace the previous expression by stk for some $s \in S$, $t \in T$, and k in some set of coset representatives of $K \cap H$ in K.

Again let $[\alpha_1, \ldots, \alpha_r]$ be a minimal factorisation for H and $[\beta_1, \ldots, \beta_s]$ be a minimal factorisation for K over K_1. Consider the sequence $\gamma = [\alpha_1, \ldots, \alpha_r, S, T, \beta_2, \ldots, \beta_s]$. The previous paragraph shows that γ is a logarithmic signature for G. By (2), we have $\mathcal{B}(G) = p + q + \mathcal{B}(H) + \mathcal{B}(K) - \mathcal{B}(K_1)$, which is the length of γ. So γ is a minimal factorisation for G. □

3. MINIMAL FACTORISATIONS OF SOME SPORADICS

Our permutation representations and some words for subgroups come from the electronic ATLAS [Wilson et al. 04]. All calculations in permutation groups are done in Magma [Bosma and Canon 95]. Possible candidates for factorisation subgroups were found using the ATLAS [Conway et al. 85] and GAP's character table library [Schönert 94].

When we need random(ish) elements of our groups we use the words given in Figure 1.

To save space, we denote the product $\phi_i(g,h)\phi_j(g,h)$ by $\phi_{i,j}(g,h)$.

3.1 J_1

We factorise J_1 using Condition 2.6. We let H be the subgroup $L_2(11)$ and take K to be a cyclic group of order 19.

Let a and b be images of standard generators (see [Wilson 96]) of J_1 in the permutation representation on the 266 cosets of $L_2(11)$. The element $\phi_5(a,b)$ has order 19. Let λ be the set of 14 orbits of $K = \langle \phi_5(a,b) \rangle$ and let

$$\begin{array}{lll} t_1 = \phi_2(a,b) & t_2 = \phi_{21}(a,b) & t_3 = \phi_{21,2}(a,b) \\ t_4 = \phi_{5,7}(a,b) & t_5 = \phi_{22,10}(a,b) & t_6 = \phi_{22,11}(a,b) \\ t_7 = Id(J_1). & & \end{array}$$

We can choose a pair of points p_1 and p_2 so that each of the points $p_i^{t_j}$ is in a distinct K-orbit for $1 \leq i \leq 2$ and $1 \leq j \leq 7$. (When using the representation obtained from [Wilson et al. 04] we have $p_1 = 1$ and $p_2 = 262$.) Let H be any copy of $L_2(11) \leq J_1$. By the transitivity of

$$\begin{array}{rclcrcl}
\phi_1(g,h) & = & g & & \phi_{12}(g,h) & = & \phi_3(g,h)\phi_{11}(g,h)\\
\phi_2(g,h) & = & h & & \phi_{13}(g,h) & = & \phi_{12}(g,h)\phi_3(g,h)\\
\phi_3(g,h) & = & gh & & \phi_{14}(g,h) & = & \phi_{13}(g,h)\phi_4(g,h)\\
\phi_4(g,h) & = & gh^2 & & \phi_{15}(g,h) & = & \phi_{14}(g,h)\phi_4(g,h)\\
\phi_5(g,h) & = & ghgh^2 & & \phi_{16}(g,h) & = & \phi_5(g,h)\phi_{15}(g,h)\\
\phi_6(g,h) & = & (gh)^2gh^2 & & \phi_{17}(g,h) & = & \phi_{16}(g,h)\phi_5(g,h)\\
\phi_7(g,h) & = & (gh)^2gh^2gh & & \phi_{18}(g,h) & = & \phi_{17}(g,h)\phi_3(g,h)\\
\phi_8(g,h) & = & gh(ghgh^2)^2 & & \phi_{19}(g,h) & = & \phi_4(g,h)\phi_{18}(g,h)\\
\phi_9(g,h) & = & (gh)^2(ghgh^2)^2 & & \phi_{20}(g,h) & = & \phi_{19}(g,h)\phi_3(g,h)\\
\phi_{10}(g,h) & = & (gh)^2(ghgh^2)^2gh^2 & & \phi_{21}(g,h) & = & \phi_{14}(g,h)\phi_{15}(g,h)\\
\phi_{11}(g,h) & = & \phi_{10}(g,h)\phi_4(g,h) & & \phi_{22}(g,h) & = & \phi_9(g,h)\phi_{12}(g,h)
\end{array}$$

FIGURE 1.

J_1 on the cosets of H, we can find a pair of elements s_1 and s_2 mapping the fixed point of H to points p_1 and p_2 respectively.

By [Magliveras 02], a minimal factorisation exists for all $\mathrm{PSL}_2(q)$, so H has a minimal factorisation. The intersection of K and H is trivial, so all points are fixed by $K \cap H$, and as K is cyclic it has a minimal factorisation (see [Magliveras 02]). By the previous paragraph the sequences $S = [s_1, s_2]$ and $T = [t_1, \ldots, t_7]$ satisfy the requirements for S and T in Condition 2.6, so J_1 has a minimal factorisation.

3.2 J_2

We show that J_2 satisfies Condition 2.3 and therefore has a minimal factorisation.

We let the subgroups $\mathrm{U}_3(3)$ play the role of H in Condition 2.3, we let K be a Sylow 5-subgroup, and let K_1 be the trivial group.

The subgroup H has index $100 = 4|K|/|K_1|$ in J_2. There are no elements of order 5 in $\mathrm{U}_3(3)$ so K acts on the cosets of H in J_2 with four regular orbits, each of length 25. From [Vasco et al. 03] we know that $\mathrm{U}_3(3)$ has a minimal factorisation, and so do all soluble groups (including K), so Condition 2.3 is satisfied.

3.3 HS

This case is similar to the previous one. We let H be a subgroup M_{22} of HS, K be a 5A-pure elementary abelian subgroup of order 25 and K_1 be trivial.

Again we have $|\mathrm{HS}| = 4|\mathrm{M}_{22}||K|/|K_1|$. All the elements of order 5 in M_{22} are in class 5B in HS so the orbits of K on the cosets of H in HS are regular. From [Vasco et al. 03] we know that M_{22} has a minimal factorisation, and so does K as it is soluble. So HS satisfies Condition 2.3 and therefore has a minimal factorisation.

3.4 M$^{\mathrm{c}}$L

First we use Conditions 2.3 and 2.4 to show that the subgroup $\mathrm{U}_4(3)$ of M$^{\mathrm{c}}$L has a minimal factorisation. This allows us to use Condition 2.6 to show that M$^{\mathrm{c}}$L has a minimal factorisation, with $H \cong \mathrm{U}_4(3)$ and K a cyclic group of order 11.

To show that $\mathrm{U}_4(3)$ has a minimal factorisation, we start by using Condition 2.4. We let a subgroup $\mathrm{L}_3(4)$ play the role of H. A minimal factorisation exists for $\mathrm{L}_3(4)$ as it has order less than $|\mathrm{J}_1|$ ([Vasco et al. 03]). We look for a subgroup to play the role of $|K|$ by making a copy of each maximal subgroup of $\mathrm{U}_4(3)$ with order divisible by $[\mathrm{U}_3(4) : \mathrm{L}_3(4)] = 162$. Words for each maximal subgroup in terms of standard generators are given in [Wilson et al. 04]. We found that a copy of $\mathrm{O}_5(3)$ was transitive on the 162 cosets of $\mathrm{L}_3(4)$. By Condition 2.4, it is now enough to show that $\mathrm{O}_5(3)$ has a minimal factorisation over $\mathrm{O}_5(3) \cap \mathrm{L}_3(4)$.

The intersection $\mathrm{O}_5(3) \cap \mathrm{L}_3(4)$ has order 160 and therefore has trivial intersection with all Sylow 3-subgroups of $\mathrm{O}_5(3)$. A Sylow 3-subgroup has order 81 and therefore has two regular orbits on the 162 points. We can then use Condition 2.3 (with the Sylow 3-subgroup as K and the trivial group as K_1) to prove that $\mathrm{O}_5(3)$ has a minimal factorisation over $\mathrm{O}_5(3) \cap \mathrm{L}_3(4)$. This completes the minimal factorisation of $\mathrm{U}_4(3)$.

Now we show that our minimal factorisation for $\mathrm{U}_4(3)$ implies the existence of one for M$^{\mathrm{c}}$L. We use the permutation representation on the 275 cosets of $H \cong \mathrm{U}_4(3)$ on standard generators a and b given in [Wilson et al. 04]. The element $x = ab$ has order 11 and is fixed point free in this representation, so we let $K = \langle x \rangle$ and note that $K \cap H$ is trivial. The element $y = b^a$ has order 5 and we can find a set λ consisting of five of its orbits, whose union contains one point from each orbit of $\langle ab \rangle$, so the sequence $[y^1, \ldots, y^5]$ satisfies the requirements for T in the condition. By transitivity of G on the cosets of

H there exists a sequence $S = [s_1, \dots, s_5]$ mapping the fixed point of H into each orbit in λ.

As K is cyclic it has a minimal factorisation over the trivial group, and we proved above that $\mathrm{U}_4(3)$ has one. So M^cL satisfies Condition 2.6 and therefore has a minimal factorisation.

3.5 Co_3

We use Condition 2.6 again to show that Co_3 has a minimal factorisation.

We will let H be the subgroup $\mathrm{M^cL}{:}2$. The proof that $\mathrm{M^cL}$ has a minimal factorisation is given above, so by Condition 2.1 the group $\mathrm{M^cL}{:}2$ also has one.

Now let a and b be the standard generators for Co_3 on the 276 cosets of H points given in [Wilson et al. 04]. The element $y = \phi_{7,12}(a, b)$ has order 23 and is fixed point free so we let $K = \langle y \rangle$. We find a sequence T of four elements

$$x_1 = Id(\mathrm{Co}_3), \qquad x_2 = \phi_8(a, b),$$
$$x_3 = \phi_{15}(a, b), \qquad \text{and} \quad x_4 = \phi_{13,2}(a, b)$$

and a 3-point set ω such that $\cup_{i=1}^{4} \omega^{x_i}$ meets every orbit of $\langle y \rangle$ once. In the electronic ATLAS [Wilson et al. 04] representation we have $\omega = \{1, 185, 245\}$. A sequence S of three elements mapping one to each point of ω must exist by the transitivity of Co_3 on the cosets of H.

The subgroup K is cyclic and so has a minimal factorisation over the trivial subgroup $K \cap H$ and above we showed that H has a minimal factorisation. So Co_3 has a minimal factorisation by Condition 2.6.

3.6 He

First we show that the group $\mathrm{S}_4(4)$ has a minimal factorisation. It has a subgroup H of order 23040 and index 85. The order of H is less than $|\mathrm{J}_1|$ so H has a minimal factorisation, and as 17 does not divide $|H|$ we can choose a subgroup K of order 17 so that $\mathrm{S}_4(4)$ satisfies Condition 2.3. By Condition 2.1, if $\mathrm{S}_4(4)$ has a minimal factorisation then so does $\mathrm{S}_4(4){:}2$.

So to prove that He has a minimal factorisation it suffices to prove that it has one over the maximal subgroup $\mathrm{S}_4(4){:}2$. We use Condition 2.3 with $H \cong \mathrm{S}_4(4){:}2$.

The 7-local subgroup $7^{1+2}{:}(3 \times \mathrm{S}_3) \leq$ He has two orbits of length 1029 on the 2058 cosets of H, and there is a subgroup $K_1 \leq 7^{1+2}{:}(3 \times \mathrm{S}_3)$ of order 6 that stabilises a point in both orbits. The group $7^{1+2}{:}(3 \times \mathrm{S}_3)$ has a minimal factorisation over K_1 by Condition 2.3 as its order is $3|K_1||7^{1+2}|$. So He satisfies Condition 2.3.

3.7 Ru

We checked all pairs of maximal subgroups of Ru using the words for maximal subgroups from [Wilson et al. 04]. We found that one factorisation of Ru is $\mathrm{Ru} \cong {}^2\mathrm{F}_4(2)\mathrm{L}_2(29)$. The intersection of $\mathrm{L}_2(29)$ and ${}^2\mathrm{F}_4(2)$ has order 3. We can find a minimal factorisation for $\mathrm{L}_2(29)$ over a subgroup of order 3 via a dihedral subgroup H of order 30. There is a minimal factorisation of H over a subgroup of order 3, and we can find a subgroup $K \cong 29{:}14$ with $|\mathrm{L}_2(29)| = 2|K||H|$. So by Condition 2.4 a minimal factorisation exists for Ru if we can find one for ${}^2\mathrm{F}_4(2)$.

3.8 Suz

We show that Suz has a minimal factorisation over $\mathrm{G}_2(4)$. So the existence of a minimal factorisation of $\mathrm{G}_2(4)$ would imply the existence of one for Suz.

The 3-local subgroup $3^5{:}\mathrm{M}_{11}$ acts transitively on cosets of $G_2(4)$ with point stabiliser $3^{\cdot}\mathrm{A}_6$. This action is imprimitive, with block stabiliser $3^{5\cdot}\mathrm{M}_{10}$. The block stabiliser factorises over the point stabiliser as $3^{\cdot}\mathrm{A}_6.3^4.2$ and the block stabiliser has index 11 in $3^5{:}\mathrm{M}_{11}$. This gives a minimal factorisation for $3^5{:}\mathrm{M}_{11}$ over $3^5{:}\mathrm{M}_{11} \cap \mathrm{G}_2(4)$, so a factorisation of $\mathrm{G}_2(4)$ would allow Suz to fulfil Condition 2.4.

4. CONCLUSIONS

We have given some new conditions for the existence of minimal factorisations. Armed with these conditions we have proved that minimal factorisations exist for the sporadic groups J_1, J_2, HS, M^cL, He, and Co_3. We also reduce the problem of finding minimal factorisations of Ru and Suz to that of finding one for the groups ${}^2\mathrm{F}_4(2)$ and $\mathrm{G}_2(4)$.

ACKNOWLEDGMENTS

The author would like to thank the Royal Society for their financial support in the form of a Dorothy Hodgkin fellowship. She would also like to thank Rob Wilson for helpful conversations.

REFERENCES

[Bosma and Canon 95] W. Bosma and J.J. Cannon. *Handbook of Magma Functions.* School of Mathematics and Statistics, Sydney: University of Sydney, 1995.

[Conway et al. 85] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson. *Atlas of Finite Groups.* Oxford, UK: Clarendon Press, 1985.

[Vasco et al. 03] M.I. González Vasco, M. Rötteler, and R. Steinwandt. "On Minimal Length Factorizations of Finite Groups." *J. Exp. Math.* 12:1 (2003), 1–12.

[Magliveras 02] S.S. Magliveras "Secret- and Public-Key Cryptosystems from Group Factorizations." In *Cryptology*, edited by K. Nemoga and O. Grošek, Tatra Mountains Math. Pub. 25, pp. 11–22. Bratislava: Mathematical Institute of Slovak Academy of Sciences, 2002.

[Schönert 94] M. Schönert et al. *GAP – Groups, Algorithms and Programming.* Aachen: Germany, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, 1994.

[Wilson 96] R.A. Wilson. "Standard Generators for Sporadic Simple Groups." *J. Algebra* 184 (1996), 505–515.

[Wilson et al. 04] R.A. Wilson *et al.* "A World-Wide-Web Atlas of Group Representations." Available from World Wide Web (http://www.mat.bham.ac.uk/atlas), 2004.

P. E. Holmes, School of Mathematics and Statistics, University of Birmingham, Edgbaston, Birmingham B15 2TT, United Kingdom (holmespe@for.mat.bham.ac.uk)

Received December 16, 2003; accepted in revised form August 17, 2003.