Finding hidden Borel subgroups of the general linear group

Gábor Ivanyos
Computer and Automation Research Institute
of the Hungarian Academy of Sciences,
Kende u. 13-17, H-1111, Budapest, Hungary
E-mail: Gabor.Ivanyos@sztaki.hu

January 24, 2012

Abstract

We present a quantum algorithm for solving the hidden subgroup problem in the general linear group over a finite field where the hidden subgroup is promised to be a conjugate of the group of the invertible lower triangular matrices. The complexity of the algorithm is polynomial when size of the base field is not much smaller than the degree.

1 Introduction

The hidden subgroup problem (HSP for short) is the following. We are given a black box function f on a group $\mathcal{G}$ such that there is a subgroup $\mathcal{H}$ of $\mathcal{G}$ satisfying $f(x) = f(y)$ if and only if x and y are in the same right coset of $\mathcal{H}$ (that is, $yx^{-1} \in \mathcal{H}$). The task is to determine the subgroup $\mathcal{H}$, which is unique and called the subgroup hidden by f. Computing orders of elements of groups, calculating discrete logarithms and even finding isomorphisms between graphs can be cast in the paradigm of the HSP [19].

On classical computers, the query complexity of the hidden subgroup problem is exponential (in $\log |\mathcal{G}|$) already over finite commutative groups. In the quantum setting f is assumed to be given by a quantum oracle which is a unitary map U_f mapping states of the form $|x\rangle|0\rangle$ to $|x\rangle|f(x)\rangle$. In contrast to the classical case the quantum query complexity of the HSP is polynomial (in $\log |\mathcal{G}|$), see [10]. Furthermore, there are polynomial time quantum algorithms [5, 20] solving the hidden subgroup problem in abelian groups, generalizing Shor's result on order finding and computing discrete logarithm [23]. Computing the structure of finite commutative black box groups [7] is a more general application of the abelian HSP.

As the graph isomorphism problem is involved, in the past decade considerable efforts have been spent on finding efficient algorithms for noncommutative cases of the HSP. Although nice results have been achieved in this direction, the groups in which the HSP can be solved at present in quantum polynomial time remain actually very close to being commutative. One of the widest classes of finite groups in which the HSP is known to have a polynomial time quantum solution consists of solvable groups whose derived subgroup have of constant derived length and constant exponent [11]. Other classes of groups with efficient quantum HSP algorithms include certain "almost Hamiltonian" groups [12] and two-step nilpotent groups [18]. The latter class contains Heisenberg groups for which efficient HSP algorithms are also given in [2] and [1]. The "pretty good measurement" technique of [2] actually works also in certain nilpotent semidirect product groups of higher nilpotency class. An efficient HSP algorithm is given in [16] for a special family of groups which possess a large commutative subgroup and a map transforming the HSP of the whole group to the HSP of the abelian subgroup. The limited success in finding good noncommutative HSP algorithms indicates that the problem may be actually difficult. The connection between the HSP in dihedral groups and some supposedly difficult lattice problem exposed in [22] provides further evidence for that.

Putting restrictions on the class of the possible hidden subgroups can result in efficient algorithms for finding them even in fairly noncommutative groups. Most importantly, the HSP for normal subgroups can be solved in quantum polynomial time in groups for which efficient quantum Fourier transforms exist (see [14] and [15]) and in a class of groups including solvable groups and more [17]. The methods of [21] and [13] work efficiently for sufficiently large non-normal hidden subgroups in certain semidirect products.

The first polynomial time algorithm for finding special hidden subgroups in simple and almost simple groups is given in [8]. (An almost simple group has a large noncommutative simple constituent.) The main result of Ibid. is an efficient quantum algorithm that solves the HSP in the group of 2 by 2 invertible matrices (and related groups) where the hidden subgroup is promised to be a *Borel subgroup* (definition will be given below). In this paper generalize this result to finding hidden Borel subgroups in general linear groups of higher degree.

We denote by $\mathrm{GL}_n(\mathbf{F}_q)$ the general linear group consisting of the invertible $n \times n$ matrices over the finite field $\mathbf{F}_q$ having q elements. We propose a quantum algorithm for the HSP in $\mathrm{GL}_n(\mathbf{F}_q)$ where the hidden subgroup is promised to be a Borel subgroup. For brevity we use the term *hidden Borel subgroup problem* for this promise problem. Our algorithm works in polynomial time if q is not much smaller than n.

A Borel subgroup of $\mathrm{GL}_n(\mathbf{F}_q)$ is a conjugate of the subgroup consisting of the invertible lower triangular matrices (see [24]). An alternative definition for a Borel subgroup is being the stabilizer in $GL_n(\mathbf{F}_q)$ of a flag $\mathbf{F}_q^n > U_1 > U_2 > \ldots > U_{n-1} > (0)$ of subspaces of the space $V = \mathbf{F}^n$ of the column vectors of length n. Indeed, for $0 < k < n$ let V_k be the set of column vectors whose first k entries are zero. Then the invertible lower triangular matrices A form the stabilizer of the flag $\mathbf{F}_q^n > V_1 > V_2 > \ldots > V_{n-1} > (0)$, and their conjugates $X^{-1}AX$ by X form the stabilizer of the flag $\mathbf{F}_q^n > X^{-1}V_1 > X^{-1}V_2 > \ldots > X^{-1}V_{n-1} > (0)$.

To fix a nicely defined output, by solving the hidden Borel subgroup problem we mean determining the flag of subspaces stabilized by the hidden Borel subgroup. We remark that, given such a flag, it is easy to construct generators for its stabilizer.

Our method (described in Section 3) is based on the observation that a coset of a Borel subgroup is quite a large subset of a linear space of n by n matrices. The main technical tool is a version of the standard algorithm for the abelian HSP, adapted to linear spaces (see Section 2). In Section 4 we show how to extend our result to finding hidden Borel subgroups of the special linear group.

2 The quantum Fourier transform for linear spaces

In this section we briefly overview the main ingredient of the standard method for solving the hidden subgroup problem in $\mathbf{F}_q^m$ where the hidden subgroup is promised to be an $\mathbf{F}_q$-linear subspace W of $\mathbf{F}_q^m$ and give an interpretation of the result in the special case of a linear space of matrices.

The procedure receives a superposition

$$\frac{1}{\sqrt{|W|}} \sum_{v \in W} |v + v_0\rangle \tag{1}$$

over a coset $W + v_0$ and obtains information on W using the quantum Fourier transform (QFT) of the group $\mathbf{F}_q^m$. Here we use a version which is the m'th tensor power of the QFT defined in [9] for $\mathbf{F}_q$. This transform maps a $|x\rangle$ ($x \in \mathbf{F}_q$) to

$$\frac{1}{\sqrt{q}} \sum_{y \in \mathbf{F}_q} \omega^{\mathrm{Tr}(xy)} |y\rangle$$

where Tr is the trace map from $\mathbf{F}_q$ to $\mathbf{F}_p$ and ω is the primitive p'th root of unity $e^{\frac{2\pi i}{p}}$. (Here p is the prime such that $q = p^r$ for a positive integer r and the trace map is defined as $\mathrm{Tr}(x) = \sum_{i=0}^{r-1} x^{p^r}$.) By Lemma 2.2 of [9], this map has a polynomial time approximate implementation on a quantum computer, therefore its m'th tensor power can be efficiently approximated as well. The image of $|x\rangle$ for a vector $x = (x_1, \ldots, x_m)^T \in \mathbf{F}_q^m$ under the tensor power map is

$$\frac{1}{q^{m/2}} \sum_{y \in \mathbf{F}_q^m} \omega^{\mathrm{Tr}(x,y)} |y\rangle,$$

where (x, y) stands for the standard scalar product $x^T y = \sum_{i=1}^m x_i y_i$ on $\mathbf{F}^m$. Our input superposition (1) gets mapped to the state

$$\sum_{y \in \mathbf{F}^m} c_y |y\rangle,$$

where

$$c_y = \frac{\omega^{(v_0,y)}}{\sqrt{|W| q^m}} \sum_{v \in W} \omega^{(v,y)}.$$

The subspace $W^\perp$ consisting of the vectors u from $\mathbf{F}_q^m$ such that $(u,v)=0$ for every $v \in W$ has dimension $m - \dim_{\mathbf{F}_q} W$, therefore $|W^\perp| = \frac{q^m}{|W|}$. For $y \in W^\perp$ we have

$$|c_y| = \frac{1}{\sqrt{|W|q^m}} \sum_{v \in W} \omega^0 = \frac{|W|}{\sqrt{|W|q^m}} = \frac{1}{\sqrt{|W^\perp|}}.$$

It follows that

$$\sum_{y \in W^\perp} |c_y|^2 = |W^\perp| \cdot \frac{|1|}{|W^\perp|} = 1.$$

Therefore for $y \notin W^\perp$ we have $c_y = 0$ and if we measure $|y\rangle$, we obtain a uniformly random element of $W^\perp$.

Assume now that $\mathcal{W}$ is a subspace of the linear space $\mathcal{M}_{n\times n}(\mathbf{F}_q)$ of $n \times n$ matrices over $\mathbf{F}_q$. We can consider $n \times n$ matrices as vectors of length n^2. Then the standard scalar product of two matrices $A = (a_{ij})$ and $B = (b_{ij})$ is

$$\sum_{i,j=1}^{n} a_{ij} b_{ij} = \mathrm{tr}(AB^T).$$

Here, for a matrix $D \in \mathcal{M}_{n\times n}(\mathbf{F}_q)$, by $\mathrm{tr}(D)$ we denote the sum of the diagonal elements of D. (Thus $\mathrm{tr}(D)$ is an element of $\mathbf{F}_q$. The map tr from $\mathcal{M}_{n\times n}(\mathbf{F}_q)$ to $\mathbf{F}_q$ should not be confused with the trace map Tr from $\mathbf{F}_q$ to $\mathbf{F}_p$, although they are not completely unrelated.) We will make use of the identity $\mathrm{tr}(XY) = \mathrm{tr}(YX)$.

3 Finding hidden Borel subgroups in the general linear group

In this section we outline a quantum algorithm for finding a hidden Borel subgroup $\mathcal{H}$ in the group $\mathrm{GL}_n(\mathbf{F}_q)$. Like the most hidden subgroup algorithms, our procedure is based on using superpositions over cosets of $\mathcal{H}$, that is, states of the form

$$|\mathcal{H}B\rangle = \frac{1}{\sqrt{|\mathcal{H}|}} \sum_{A \in \mathcal{H}} |AB\rangle,$$

where B is a matrix from $\mathrm{GL}_n(\mathbf{F}_q)$. We will think of such a superposition as an approximation of a superposition over a linear space of matrices and apply the quantum Fourier transform of the linear space $\mathcal{M}_{n\times n}(\mathbf{F}_q)$ to obtain a guess for the one-dimensional subspace in the flag stabilized by $\mathcal{H}$. The guess will be verified in a straightforward way. If the guess turns out to be correct, the further members of the flag can be obtained by recursion.

3.1 Obtaining coset superpositions

The standard approaches to the hidden subgroup problem in a group $\mathcal{G}$ start with the the state $\frac{1}{\sqrt{|\mathcal{G}|}} \sum_{x \in \mathcal{G}} |x\rangle|0\rangle$, apply the oracle for the function f to obtain $\frac{1}{\sqrt{|\mathcal{G}|}} \sum_{x \in \mathcal{G}} |x\rangle|f(x)\rangle$, and finally measure the second register to obtain the coset superposition

$$\frac{1}{\sqrt{|\mathcal{H}|}} \sum_{x \in \mathcal{H}} |xy\rangle$$

with some $y \in \mathcal{G}$ ($\mathcal{H}$ is the subgroup hidden by the function f). If $\mathcal{G}$ is abelian then the uniform superposition $\frac{1}{\sqrt{|\mathcal{G}|}} \sum_{x \in \mathcal{G}} |x\rangle$ over $\mathcal{G}$ can be obtained by applying the quantum Fourier transform of $\mathcal{G}$ to $|0\rangle$ (here 0 stands for the neutral element of $\mathcal{G}$). There are efficient methods for computing uniform superpositions of certain further classes of groups, e.g., the algorithm of Watrous [25] for solvable groups.

For the purposes of our algorithm it will be sufficient to approximate the uniform superposition $\frac{1}{\sqrt{|\mathrm{GL}_n(\mathbf{F}_q)|}} \sum_{x \in \mathrm{GL}_n(\mathbf{F}_q)} |x\rangle$ over the group $\mathrm{GL}_n(\mathbf{F}_q)$ by the uniform superposition $\frac{1}{\sqrt{|\mathcal{M}_{n\times n}(\mathbf{F}_q)|}} \sum_{x \in \mathcal{M}_{n\times n}(\mathbf{F}_q)} |x\rangle$ over $\mathcal{M}_{n\times n}(\mathbf{F}_q)$, which can be efficiently computed using the quantum Fourier transform of $\mathbf{F}_q^{n^2}$. The fidelity between the two states is

$$c = \sqrt{\frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{|\mathcal{M}_{n\times n}(\mathbf{F}_q)|}} = \sqrt{\frac{\prod_{i=0}^{n-1}(q^n - q^i)}{q^{n^2}}} = \sqrt{\prod_{j=1}^{n}(1 - q^{-j})} > \sqrt{\prod_{j=1}^{\infty}(1 - 2^{-j})} > \frac{1}{2}.$$

(Recall that the fidelity between two pure states is just the absolute value of their inner product.) We extend f (and the oracle U_f) to $\mathcal{M}_{n\times n}(\mathbf{F}_q)$ so that f takes a distinguished value D on non-invertible matrices. If we apply the extended oracle U_f to the superposition

$$\frac{1}{\sqrt{|\mathcal{M}_{n\times n}(\mathbf{F}_q)|}} \sum_{x \in \mathcal{M}_{n\times n}(\mathbf{F}_q)} |x\rangle|0\rangle$$

we obtain the sate

$$c \cdot \frac{1}{\sqrt{|\mathrm{GL}_n(\mathbf{F}_q)|}} \sum_{x \in \mathrm{GL}_n(\mathbf{F}_q)} |x\rangle|f(x)\rangle + \sqrt{1 - c^2}|\psi\rangle|D\rangle,$$

where

$$|\psi\rangle = \frac{1}{\sqrt{|\mathcal{M}_{n\times n}(\mathbf{F}_q) \setminus \mathrm{GL}_n(\mathbf{F}_q)|}} \sum_{x \in \mathcal{M}_{n\times n}(\mathbf{F}_q)\setminus \mathrm{GL}_n(\mathbf{F}_q)} |x\rangle.$$

Then, if we measure the second register, we find D in it with probability $1 - c^2$, while with probability $c^2 > \frac{1}{4}$, we find one of the legitimate values for the original function f and obtain a superposition over a coset of the hidden subgroup $\mathcal{H}$ in $\mathrm{GL}_n(\mathbf{F}_q)$ in the first register.

3.2 Guessing the smallest subspace in the flag

Recall that our assumption is that there exists an $n \times n$ invertible matrix X such that $\mathcal{H} = X^{-1}\mathcal{L}X$, where

$$\mathcal{L} = \{A = (a_{ij}) \in \mathrm{GL}_n(\mathbf{F}_q) : a_{ij} = 0 \text{ when } i < j\}.$$

Then the smallest nontrivial member U_{n-1} of the flag $\mathbf{F}_q^n > U_1 > \ldots > U_{n-1} > (0)$ stabilized by $\mathcal{H}$ is $X^{-1}V_{n-1}$, where V_{n-1} consists of the column vectors from $\mathbf{F}_q^n$ whose first $n-1$ entries are zero.

We will consider the multiplicative group $\mathcal{L}$ as an approximation of the subspace

$$\mathcal{L}' = \{A = (a_{ij}) \in \mathcal{M}_{n\times n}(\mathbf{F}_q) : a_{ij} = 0 \text{ when } i < j\}$$

of lower triangular matrices. Then $\mathcal{H}$ will be thought of as an approximation of $\mathcal{H}' = X^{-1}\mathcal{L}X$. We have $|\mathcal{H}| = |\mathcal{L}| = (q-1)^n q^{n(n-1)/2}$ and $|\mathcal{H}'| = |\mathcal{L}'| = q^{n(n+1)/2}$.

Accordingly, for every $B \in \mathrm{GL}_n(\mathbf{F}_q)$, the coset superposition

$$|\mathcal{H}B\rangle = \frac{1}{\sqrt{|\mathcal{L}|}} \sum_{A\in\mathcal{L}} |X^{-1}AXB\rangle$$

will be considered as an approximation of

$$|\mathcal{H}'B\rangle = \frac{1}{\sqrt{|\mathcal{L}|'}} \sum_{A\in\mathcal{L}'} |X^{-1}AXB\rangle.$$

The fidelity between $|\mathcal{H}B\rangle$ and $|\mathcal{H}'B\rangle$ is

$$\frac{\sqrt{|\mathcal{H}B|}}{\sqrt{|\mathcal{H}'B|}} = \frac{\sqrt{|\mathcal{H}|}}{\sqrt{|\mathcal{H}'|}} = \left(\frac{q-1}{q}\right)^{\frac{n}{2}}.$$

Therefore, if we apply the quantum Fourier transform of $\mathcal{M}_{n\times n}(\mathbf{F}_q)$ discussed in the previous section to the coset superposition $|\mathcal{H}B\rangle$, and do the measurement then, with a chance at least $\Omega\left(\left(\frac{q-1}{q}\right)^n\right)$, the result will be a uniformly random element of the subspace $(\mathcal{H}'B)^\perp$, as it would be the case when we started with the state $|\mathcal{H}'B\rangle$. (Our state before the measurement we may have an error term of amplitude $\sqrt{1-\Omega\left(\left(\frac{q-1}{q}\right)^n\right)}$ orthogonal to the "ideal" state and hence after the measurement with probability $1-\Omega\left(\left(\frac{q-1}{q}\right)^n\right)$ we may get a false or even meaningless result.)

Let Y be a matrix from $\mathcal{M}_{n\times n}(\mathbf{F}_q)$. Then $Y \in (\mathcal{H}'B)^\perp = (X^{-1}\mathcal{L}'XB)^\perp$ if and only if $\mathrm{tr}(X^{-1}AXBY^T) = 0$ for every $A \in \mathcal{L}'$. As

$$\mathrm{tr}\left(X^{-1}AXBY^T\right) = \mathrm{tr}\left(AXBY^TX^{-1}\right) = \mathrm{tr}\left(A\left((X^T)^{-1}YB^TX^T\right)^T\right),$$

we obtain that $Y \in (\mathcal{H}'B)^\perp$ if and only if $(X^T)^{-1}YB^TX^T \in \mathcal{L}'^\perp$. Furthermore, as multiplying matrices by B^T and conjugating matrices by X^T are bijections, we can conclude that if Y is a uniformly random element of $(\mathcal{H}'B)^\perp$ then $(X^T)^{-1}YBX^T$ is a uniformly random element of $\mathcal{L}'^\perp$. Observe that the elements of $\mathcal{L}'^\perp$ are just the strictly upper triangular $n \times n$ matrices. A strictly upper triangular matrix Z has rank $n-1$ if and only if all the entries of Z just above the principal diagonal are nonzero. For a uniformly random strictly upper triangular matrix this happens with probability $\left(\frac{q-1}{q}\right)^{n-1} > \left(\frac{q-1}{q}\right)^n$.

Observe that if Z is a strictly upper triangular matrix of rank $n-1$ then the kernel of Z^T is the set V_{n-1} of column vectors from $\mathbf{F}^n$ whose first $n-1$ entries are zero. Obviously, the matrix $(X^T)^{-1}YB^TX^T$ has the same rank as Y. If the rank is $n-1$, then the kernel of $XBY^TX^{-1} = \left((X^T)^{-1}YBX^T\right)^T$ is V_{n-1}, whence the kernel of Y^T is the 1-dimensional subspace $X^{-1}V_{n-1}$, which is the one-dimensional subspace of the flag stabilized by $\mathcal{H}$.

In summary, by applying the quantum Fourier transform to the coset state $|\mathcal{H}B\rangle$ and then measuring the result, with probability $\Omega\left((1-q^{-1})^{2n}\right)$ we obtain a matrix Y of rank $n-1$ with kernel U_{n-1}.

3.3 Putting things together

In this part we show how to check and use a guess for the one-dimensional subspace U_{n-1} of the flag stabilized by the hidden Borel subgroup $\mathcal{H}$ provided by the algorithm described in the previous subsection.

As U_{n-1} is one-dimensional, we assume that the guess is given by a nonzero column vector u. Let Z be a matrix from $\mathrm{GL}_n(\mathbf{F}_q)$ whose last column is u. Then $U_{n-1} = ZV_{n-1}$. We replace the hiding function f by f' defined as $f'(A) = f(ZAZ^{-1})$. An oracle for f' can be obtained from the oracle for f in an obvious way using this definition. The subgroup hidden by f' is $Z^{-1}\mathcal{H}Z$ and the one-dimensional subspace of the flag stabilized by $Z^{-1}\mathcal{H}Z$ is $Z^{-1}U_{n-1}$. The guess for U_{n-1} is correct if and only if $Z^{-1}U_{n-1} = V_{n-1}$, that is, the subgroup $Z^{-1}\mathcal{H}Z$ hidden by f' is contained in the subgroup of matrices of the form

$$\begin{pmatrix} A & 0 \\ v & \alpha \end{pmatrix},$$

where $A \in \mathrm{GL}_{n-1}(\mathbf{F}_q)$, $\alpha \in \mathbf{F}_q \setminus \{0\}$ and v is row vector of length $n-1$. Testing correctness of the guess can be carried out by calling the oracle for the identity matrix and for the $n-1$ matrices of the form

$$\begin{pmatrix} I & 0 \\ v & 1 \end{pmatrix}$$

with $v = (1,0,0,\ldots,0)$, $(0,1,0,\ldots,0)$, …, $(0,0,\ldots,0,1)$. Note that we can obtain a correct guess with expected $O\left((1-q^{-1})^{-n}\right)$ repetitions of procedure described in the previous subsection.

Assume that the guess is correct. Then we consider the subgroup $\mathcal{G}$ of $GL_n(\mathbf{F})$ consisting

of the matrices of the form

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix},$$

with $A \in \mathrm{GL}_{n-1}(\mathbf{F}_q)$. Taking the upper left $n-1$ by $n-1$ block of matrices gives an isomorphism between $\mathcal{G}$ and $GL_{n-1}(\mathbf{F}_q)$. Furthermore, $\mathcal{G} \cap Z^{-1}\mathcal{H}Z$ is a Borel subgroup of $\mathcal{G}$. The subspaces in the flag stabilized by $\mathcal{G} \cap Z^{-1}\mathcal{H}Z$ are intersections of those for $Z^{-1}\mathcal{H}Z$ with the subspace of the column vectors with zero as last entry. We determine this flag by recursion. Then we obtain the flag for $Z^{-1}\mathcal{H}Z$ by adding U_{n-1} to each of the members. Finally the complete flag for $\mathcal{H}$ is obtained by applying Z.

The group $\mathrm{PGL}_n(\mathbf{F}_q)$ is the factor of $\mathrm{GL}_n(\mathbf{F}_q)$ by its center consisting of the scalar matrices and the Borel subgroups of $\mathrm{PGL}_n(\mathbf{F}_q)$ are just the images of the Borel subgroups of $\mathrm{GL}_n(\mathbf{F}_q)$ under the quotient map. As the scalar matrices from $\mathrm{GL}_n(\mathbf{F}_q)$ are contained in every Borel subgroup, the hidden Borel subgroup problem for the groups $\mathrm{PGL}_n(\mathbf{F}_q)$ and $\mathrm{GL}_n(\mathbf{F}_q)$ essentially coincide. (A function hiding a Borel subgroup of $\mathrm{PGL}_n(\mathbf{F}_q)$ can be lifted to $\mathrm{GL}_n(\mathbf{F}_q)$ in the straightforward way.) We have proved the following.

Theorem 1 *The hidden Borel subgroup problem in* $\mathrm{GL}_n(\mathbf{F}_q)$ *(and in* $\mathrm{PGL}_n(\mathbf{F}_q)$*) can be solved in quantum time* $\mathrm{poly}(n + \log q + (1-q^{-1})^{-n})$.

4 Finding Borel subgroups in the special linear group

The special linear group $\mathrm{SL}_n(\mathbf{F}_q)$ consists of n by n matrices over $\mathbf{F}_q$ with determinant one. In this section we briefly outline an extension of our method to finding hidden Borel subgroups in $\mathrm{SL}_n(\mathbf{F}_q)$. A Borel subgroup of $\mathrm{SL}_n(\mathbf{F}_q)$ is just the intersection of $\mathrm{SL}_n(\mathbf{F}_q)$ with a Borel subgroup of $\mathrm{GL}_n(\mathbf{F}_q)$, that is, the stabilizer of a flag $\mathbf{F}_q^n > U_1 > \ldots > U_{n-1} > (0)$ of subspaces within $\mathrm{SL}_n(\mathbf{F}_q)$. Again, we require the output of the HSP algorithm to be this flag.

Assume that we have a function f defined on $\mathrm{SL}_n(\mathbf{F}_q)$ that hides a conjugate of the subgroup $\mathcal{L}_0$ consisting of the lower triangular matrices having determinant 1. Let $\mathcal{G}$ stand for the subgroup of $\mathrm{GL}_n(\mathbf{F}_q)$ consisting of matrices whose determinant are from $\mathbf{F}_q^{*n}$, where $\mathbf{F}_q^{*n} = \{x^n : 0 \neq x \in \mathbf{F}_q\}$. We extend f to $\mathcal{G}$ as follows. Let A be a matrix from $\mathcal{G}$. We compute $\det A$ and find an element $z \in \mathbf{F}_q$ such that $z^n = \det A$. Such elements z can be read from the linear factors of the polynomial $x^n - \det A$, which can be found classically in time polynomial in n and $\log q$, using the randomized method of Berlekamp [3, 4] or the even more efficient algorithm of Cantor and Zassenhaus [6]. (On a quantum computer, a simple root extracting method based on calculating discrete logarithm also does the job in polynomial time.) We put $f(A) = f(z^{-1}A)$. It turns out that the definition of $f(A)$ does not depend on the choice of z. Indeed, if $z_1^n = z^n$ then $z_1^{-1}zI$ is in the subgroup of $\mathrm{SL}_n(\mathbf{F}_q)$ hidden by f and therefore $f(z_1^{-1}A) = f(zA)$. The subgroup of $\mathcal{G}$ hidden by the extended function will be a conjugate of the lower triangular matrices with determinant from $\mathbf{F}_q^{*n}$. The fidelity between the uniform superposition over this set and the uniform superposition over all the lower triangular matrices is at least $\frac{1}{\sqrt{n}}\left(\frac{q-1}{q}\right)^{\frac{n}{2}}$. (Compared to the case of $\mathrm{GL}_n(\mathbf{F}_q)$ studied

in Section 3, we have here an extra factor $\frac{1}{\sqrt{n}}$ as $\mathcal{G}$ has index n in $\mathrm{GL}_n(\mathbf{F}_q)$.) Therefore, if we apply the method of Subsection 3.2 for guessing the one-dimensional member of the stabilized flag, we have a further factor $\Omega\left(\frac{1}{n}\right)$ for the probability of obtaining a correct guess. Testing correctness and the recursion are also essentially the same as in the case for $\mathrm{GL}_n(\mathbf{F}_q)$. We obtain the following.

Theorem 2 *The hidden Borel subgroup problem in* $\mathrm{SL}_n(\mathbf{F}_q)$ *(and in* $\mathrm{PSL}_n(\mathbf{F}_q)$*) can be solved in quantum time* $\mathrm{poly}(n + \log q + (1 - q^{-1})^{-n})$.

As $(1 - q^{-1})^{-n}$ is polynomial in n if $q = \Omega(\frac{n}{\log n})$, we have

Corollary 3 *When* $q = \Omega(\frac{n}{\log n})$*, the hidden Borel subgroup problem in* $\mathrm{GL}_n(\mathbf{F}_q)$ *and* $\mathrm{SL}_n(\mathbf{F}_q)$ *(and in* $\mathrm{PGL}_n(\mathbf{F}_q)$ *and* $\mathrm{PSL}_n(\mathbf{F}_q)$*) can be solved in quantum time* $\mathrm{poly}(n + \log q)$*. In particular, for constant* n*, the quantum complexity of the problem is* $\mathrm{poly}(\log q)$.

5 Concluding remarks

In this paper we have proved that the hidden Borel subgroup in $\mathrm{GL}_n(\mathbf{F}_q)$ and $\mathrm{SL}_n(\mathbf{F}_q)$ can be solved in quantum polynomial time if the size q of the base field is not too much smaller than the degree n. Perhaps the most important question which is left open is existence of polynomial time algorithms over small base fields (e.g., over fields of constant size).

Other interesting questions are whether it is possible to extend the result to the hidden Borel subgroup problem in other classical groups (e.g., the orthogonal groups) and if it is possible to find efficiently hidden conjugates of certain subgroups of the lower triangular matrices such as the unitriangular matrices or the diagonal matrices.

Acknowledgments The author is grateful to an anonymous referee for helpful remarks and suggestions. Part of research was conducted during the author's visit at the Centre for Quantum Technologies (CQT) in Singapore, funded by the Singapore Ministry of Education and the National Research Foundation. Research was also supported by the Hungarian Research Fund (OTKA).

References

[1] D. Bacon (2008), *How a Clebsch-Gordan transform helps to solve the Heisenberg hidden subgroup problem*, Quantum Inf. Comput., Vol. 8, pp. 438-467.

[2] D. Bacon, A. Childs, and W. van Dam (2005), *From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups*, In Proc. 46th IEEE FOCS, pp. 469-478.

[3] E. R. Berlekamp (1968), *Algebraic coding theory*, McGraw-Hill, New York.

[4] E. R. Berlekamp (1970), *Factoring polynomials over large finite fields*, Math. Comput., Vol. 24, pp. 713-735.

[5] D. Boneh and R. Lipton (1995), *Quantum cryptanalysis of hidden linear functions*, In: Proc. Crypto'95, Lect. Notes Comput. Sci., Vol. 963, Springer-Verlag (Berlin), pp. 427-437.

[6] D. G. Cantor, H. Zassenhaus (1981), *A New Algorithm for Factoring Polynomials Over Finite Field,* Math. Comput. 36, pp. 587-592.

[7] K. Cheung and M. Mosca (2001), *Decomposing finite abelian groups*, Quantum Inf. Comput., Vol. 1, pp. 26-32.

[8] A. Denney, C. Moore, and A. Russell (2010), *Finding conjugate stabilizer subgroups in PSL(2;q) and related problems*, Quantum Inf. Comput., Vol. 10, pp. 282-291.

[9] W. van Dam, S. Hallgren, and L. Ip (2006), *Quantum algorithms for some hidden shift problems*, SIAM J. Comput., Vol 36, pp 763-778.

[10] M. Ettinger, P. Hoyer, and E. Knill (2004), *The quantum query complexity of the hidden subgroup problem is polynomial*, Inform. Proc. Lett., 91, pp. 43-48.

[11] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen (2003), *Hidden translation and orbit coset in quantum computing*, In: Proc. 35th ACM STOC, pp. 1-9.

[12] D. Gavinsky (2004), *Quantum solution to the hidden subgroup problem for poly-near-Hamiltonian groups*, Quantum Inf. Comput. Vol. 4, pp. 229-235.

[13] D. N. Goncalves, R. Portugal and C. M. M. Cosme (2009), *Solutions to the hidden subgroup problem on some metacyclic groups*, In: Proc. TQC2009, Lect. Notes Comput. Sci., Vol. 5906, Springer-Verlag (Berlin), pp. 1-9.

[14] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani (2001), *Quantum mechanical algorithms for the nonabelian Hidden Subgroup Problem*, In Proc. 33rd ACM STOC, pp. 68-74.

[15] S. Hallgren, A. Russell, and A. Ta-Shma (2003), *Normal subgroup reconstruction and quantum computation using group representations*, SIAM J. Comp., 32, pp. 916-934.

[16] Y. Inui and F. Le Gall (2007), *Efficient quantum algorithms for the hidden subgroup problem over semi-direct product groups*, Quantum Inf. Comput., Vol. 7, pp. 559-570.

[17] G. Ivanyos, F. Magniez, and M. Santha (2003), *Efficient quantum algorithms for some instances of the non-Abelian hidden subgroup problem*, Int. J. Found. Comp. Sci., Vol. 15, pp. 723-739.

[18] G. Ivanyos, L. Sanselme, and M Santha (2008), *An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups*, In: Proc. LATIN 2008, Springer LNCS Lect. Notes Comput. Sci., Vol. 4957, Springer-Verlag (Berlin), pp. 759-771.

[19] R. Jozsa (2001), *Quantum factoring, discrete logarithms, and the hidden subgroup problem*, Computing in Science and Engineering, Vol. 3, pp. 34-43.

[20] A. Yu. Kitaev (1995), *Quantum measurements and the Abelian Stabilizer Problem,* Technical report arXiv:quant-ph/9511026.

[21] C. Moore, D. Rockmore, A. Russell, and L. Schulman (2004), *The power of basis selection in Fourier sampling: Hidden subgroup problems in affine groups*, In Proc. 15th ACM-SIAM SODA, pp. 1106-1115.

[22] O. Regev (2004), *Quantum computation and lattice problems*, SIAM J. Comput. 33, pp. 738-760.

[23] P. Shor (1997), *Algorithms for quantum computation: Discrete logarithm and factoring*, SIAM J. Comput., 26, pp 1484-1509.

[24] T. A. Springer (1998), *Linear Algebraic groups*, Progress in mathematics, Vol. 9, 2nd ed., Birkhäuser (Boston).

[25] J. Watrous (2001), *Quantum algorithms for solvable groups*, In Proc. 33rd ACM STOC, pp. 60-67.